

МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

КУРСОВА РОБОТА з дисципліни «Інформаційне право» на тему: «Охорона таємниці в Україні засобами кримінального права»

Здобувача 4 курсу, групи ІН19-9-22-БПр
(4,0д)

Васильчака Василя Дмитровича

Напрямок підготовки: Інформаційне право

Спеціальність: Правознавство

Керівник: Катеринчук Павло Миколайович
кандидат політичних наук, доцент

Національна шкала: _____

Кількість балів: _____

Оцінка: ECTS _____

Члени комісії _____
(підпис) (прізвище та ініціали)

(підпис) (прізвище та ініціали)

(підпис) (прізвище та ініціали)

Чернігів 2026 р.

МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

ЗАВДАННЯ

на виконання курсової роботи

Здобувача 4 курсу, групи ІН19-9-22-БПр (4,0д), Васильчака Василя Дмитровича

ТЕМА КУРСОВОЇ РОБОТИ: Охорона таємниці в Україні засобами кримінального права

Основні питання, які необхідно розкрити в курсовій роботі:

1. Поняття, ознаки та види таємниці як об'єкта правової охорони
2. Місце таємниці в системі інформаційних правовідносин
3. Нормативно-правове регулювання охорони таємниці в Україні
4. Кримінально-правова охорона державної таємниці
5. Кримінальна відповідальність за порушення таємниці приватного життя, листування, телефонних розмов та іншої кореспонденції
6. Охорона комерційної, банківської, професійної та службової таємниці засобами кримінального права
7. Проблеми кваліфікації кримінальних правопорушень, пов'язаних із розголошенням таємниці
8. Зарубіжний досвід кримінально-правової охорони таємниці
9. Шляхи вдосконалення кримінального законодавства України у сфері охорони таємниці

Керівник

Катеринчук Павло Миколайович
(кандидат політичних наук, доцент)

ЗМІСТ

ВСТУП	4
РОЗДІЛ 1 ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ОХОРОНИ ТАЄМНИЦІ В УКРАЇНІ.....	7
1.1. Поняття, ознаки та види таємниці як об'єкта правової охорони	7
1.2. Місце таємниці в системі інформаційних правовідносин	10
1.3. Нормативно-правове регулювання охорони таємниці в Україні.....	12
РОЗДІЛ 2 КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ОКРЕМИХ ВИДІВ ТАЄМНИЦІ В УКРАЇНІ	16
2.1. Кримінально-правова охорона державної таємниці.....	16
2.2. Кримінальна відповідальність за порушення таємниці приватного життя, листування, телефонних розмов та іншої кореспонденції.....	20
2.3. Охорона комерційної, банківської, професійної та службової таємниці засобами кримінального права	24
РОЗДІЛ 3 ПРОБЛЕМИ ТА НАПРЯМИ УДОСКОНАЛЕННЯ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ТАЄМНИЦІ В УКРАЇНІ	30
3.1. Проблеми кваліфікації кримінальних правопорушень, пов'язаних із розголошенням таємниці.....	30
3.2. Зарубіжний досвід кримінально-правової охорони таємниці	33
3.3. Шляхи вдосконалення кримінального законодавства України у сфері охорони таємниці	36
ВИСНОВКИ.....	41
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	44

ВСТУП

Актуальність теми дослідження зумовлена зростанням ролі інформації у сучасному суспільстві та необхідністю забезпечення належного рівня захисту відомостей, що становлять різні види таємниці. В умовах розвитку цифрових технологій, електронних комунікацій та інформаційних систем питання охорони конфіденційної інформації набуває особливого значення як для держави, так і для окремих громадян, підприємств та установ. Таємниця виступає важливим елементом правового регулювання суспільних відносин, оскільки забезпечує захист державних інтересів, приватного життя особи, комерційної діяльності та професійної інформації. Порухення режиму охорони таємниці може спричиняти значні негативні наслідки, серед яких загроза національній безпеці, порушення прав людини, економічні збитки та дестабілізація суспільних відносин.

Особливої актуальності тема набуває в умовах воєнного стану та посилення інформаційних загроз, пов'язаних із військовою агресією Російської Федерації проти України. У таких умовах державна таємниця, службова інформація та інші види захищених відомостей стають об'єктом підвищеного ризику незаконного отримання, розголошення або використання. Одночасно стрімкий розвиток інформаційних технологій та цифрового середовища створює нові способи вчинення кримінальних правопорушень, пов'язаних із порушенням режиму таємниці, що вимагає удосконалення механізмів кримінально-правового захисту. Кримінальне право у цьому контексті виконує функцію гарантування охорони суспільно значущої інформації шляхом встановлення відповідальності за незаконні дії щодо її розголошення чи використання.

Додатково слід зазначити, що сучасний етап розвитку правової системи України характеризується активною гармонізацією національного законодавства з європейськими стандартами у сфері захисту інформації та прав

людини. На практиці виникають проблеми, пов'язані з кваліфікацією кримінальних правопорушень, визначенням меж між різними видами таємниці, а також балансом між правом на доступ до інформації та необхідністю її захисту. Усе це обумовлює потребу у комплексному дослідженні охорони таємниці в Україні засобами кримінального права.

Науковці, які досліджували проблематику: Берднік І. В., Головка М. Б.; Стратонов В. М.; Сервецький І.; Teremetskyi V. I., Bandurka S. S., Korniienko M. V., Dniprov O. S., Slobodeniuk I. V., Albul S. V., Riabchenko Y. Y.; Sokurenko V., Levchenko K., Ablamskyi S., de Lima Jr O. P., Šimić G., Romaniuk V.; Благодарний А. М.; Денисовський М. Д., Томчук І. О., Сівіцька Г. Є.; Семенюк О. Г.; Ковальов К. Є., Леонов Б. Д.; Пастернак М. С.; Денищук Д. Є.; Хашев В. Г.; Сергійчук В. В.; Миргородська К., Копилов Е. В.; Антонов К. В.; Пузирний В.; Косяченко Є., Великий М., Копилов Е.; Тищенко Є. Ф.; Пащенко О. О.; Чуваков О.; Довженко В.

Мета дослідження полягає у комплексному аналізі теоретичних та практичних аспектів охорони таємниці в Україні засобами кримінального права, визначенні проблем правозастосування та обґрунтуванні напрямів удосконалення кримінально-правового механізму захисту інформації з обмеженим доступом.

Для досягнення мети були сформовані такі **завдання**:

- дослідити поняття, ознаки та види таємниці як об'єкта правової охорони
- проаналізувати місце таємниці в системі інформаційних правовідносин
- розглянути нормативно-правове регулювання охорони таємниці в Україні
- дослідити особливості кримінально-правової охорони державної таємниці
- проаналізувати кримінальну відповідальність за порушення таємниці приватного життя, листування, телефонних розмов та іншої кореспонденції
- визначити особливості охорони комерційної, банківської, професійної та службової таємниці засобами кримінального права

- виявити проблеми кваліфікації кримінальних правопорушень, пов'язаних із розголошенням таємниці
- проаналізувати зарубіжний досвід кримінально-правової охорони таємниці
- запропонувати напрями вдосконалення кримінального законодавства України у сфері охорони таємниці

Об'єктом дослідження є суспільні відносини, що виникають у сфері охорони інформації з обмеженим доступом та забезпечення її захисту засобами кримінального права.

Предметом дослідження є норми кримінального законодавства України, які регулюють охорону різних видів таємниці, а також практика їх застосування у сфері захисту інформації з обмеженим доступом.

Методи дослідження включають аналіз наукової літератури, нормативно-правових актів та судової практики, системний підхід до дослідження інформаційних правовідносин, порівняльно-правовий метод для вивчення зарубіжного досвіду, а також методи узагальнення, класифікації та логічного аналізу для визначення проблем і напрямів удосконалення кримінально-правової охорони таємниці в Україні.

Структура роботи. Робота складається зі вступу, трьох розділів, які містять дев'ять підрозділів, висновків, списку використаних джерел.

РОЗДІЛ 1

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ОХОРОНИ ТАЄМНИЦІ В УКРАЇНІ

1.1. Поняття, ознаки та види таємниці як об'єкта правової охорони

Поняття таємниці як об'єкта правової охорони формуються у межах системи права через поєднання норм конституційного, цивільного, адміністративного, кримінального та спеціального законодавства, що регулює інформаційні відносини. Інформація у правовому контексті набуває статусу об'єкта охорони у випадках, коли встановлено спеціальний режим доступу, обмеження поширення та визначено коло уповноважених осіб, яким надано право володіння або використання відповідних відомостей. Таємниця як правова категорія охоплює сукупність відомостей, доступ до яких обмежується відповідно до закону, договору або професійних обов'язків, а їх розголошення може спричинити юридичну відповідальність.

Формування інституту таємниці пов'язане з розвитком інформаційних відносин, у межах яких інформація набуває економічної, соціальної та управлінської цінності. Правовий режим таємниці виникає у зв'язку з необхідністю врегулювання доступу до відомостей, що стосуються приватної сфери особи, діяльності суб'єктів господарювання, функціонування органів державної влади та забезпечення національної безпеки [1, с.157-158]. Встановлення обмежень на поширення інформації здійснюється через нормативне закріплення категорій відомостей, порядок їх обробки, зберігання та захисту.

Поняття таємниці у праві охоплює ознаки, що відрізняють її від відкритої інформації. Перша ознака полягає у обмеженому доступі до відомостей, що визначається законом або волевиявленням власника інформації у межах дозволених правових механізмів. Друга ознака полягає у наявності спеціального правового режиму, який встановлює правила поведінки з

інформацією, включаючи порядок отримання, використання та поширення. Третя ознака полягає у юридичній захищеності інформації, що передбачає можливість застосування заходів відповідальності за її неправомірне розголошення або використання.

До системи правової охорони таємниці входять норми, що регулюють різні види інформаційних режимів. Конституційні положення визначають загальні засади охорони приватного життя та інформації про особу. Цивільно-правове регулювання охоплює питання комерційної таємниці, інтелектуальної власності та договірних зобов'язань щодо нерозголошення інформації. Кримінально-правові норми встановлюють відповідальність за незаконне отримання або поширення охоронюваних відомостей. Спеціальне законодавство деталізує режими державної, банківської, адвокатської, медичної та інших видів професійної таємниці.

Поняття таємниці як об'єкта правової охорони охоплює сукупність інформаційних ресурсів, що підлягають захисту внаслідок їх змісту, значення або суб'єктного складу. Об'єктом правового захисту виступають відомості, які мають обмежений доступ і визначений режим використання [2, с.218-219]. Юридичне значення таких відомостей полягає у можливості їх використання у господарській діяльності, управлінні, судочинстві або інших сферах суспільного життя.

Ознаки таємниці як об'єкта правової охорони охоплюють структуровані характеристики інформації. Перша ознака полягає у конфіденційності, що виражається у встановлених обмеженнях доступу до відомостей. Друга ознака полягає у наявності правового титулу охорони, який закріплює статус інформації у законодавстві або договірних відносинах. Третя ознака полягає у визначеності кола суб'єктів, які мають право доступу до відповідної інформації. Четверта ознака полягає у наявності механізмів захисту, що включають юридичні, організаційні та технічні засоби.

Види таємниці у правовій системі поділяються залежно від сфери застосування та характеру інформації. Державна таємниця охоплює відомості у

сфері оборони, зовнішньої політики, економічної безпеки та інших напрямів, розголошення яких може вплинути на функціонування держави. Режим державної таємниці встановлюється спеціальними нормативними актами та передбачає визначення ступенів секретності, порядок допуску та відповідальність за порушення режиму.

Комерційна таємниця охоплює інформацію, що використовується у господарській діяльності суб'єктів підприємництва та має економічну цінність у зв'язку з її невідомістю третім особам. До такої інформації належать виробничі технології, фінансові показники, маркетингові стратегії, клієнтські бази та інші дані, що формують конкурентні переваги. Правовий режим комерційної таємниці визначається внутрішніми документами підприємства та нормами цивільного законодавства.

Професійна таємниця охоплює відомості, отримані у зв'язку з виконанням професійних обов'язків. До цієї категорії належать адвокатська таємниця, медична таємниця, нотаріальна таємниця, банківська таємниця та інші види інформації, що виникають у процесі надання професійних послуг. Особливість цього виду полягає у тому, що обов'язок збереження інформації встановлюється законом або професійними стандартами діяльності [3, с.52-53].

Персональні дані виступають окремою категорією охоронюваної інформації, що стосується ідентифікованої або такої, що може бути ідентифікована фізичної особи. Правовий режим персональних даних передбачає обмеження їх обробки, визначення підстав для збирання, зберігання та поширення, а також гарантування прав суб'єкта даних на доступ та захист інформації.

Банківська таємниця охоплює інформацію про рахунки, операції та фінансовий стан клієнтів банківських установ. Вона захищається спеціальним законодавством, що визначає порядок доступу до таких відомостей, умови їх розкриття та відповідальність за порушення встановленого режиму. Обмеження доступу до банківської інформації пов'язане із забезпеченням стабільності фінансової системи та захистом інтересів клієнтів.

Система класифікації таємниць у праві базується на критеріях змісту інформації, суб'єктного складу та рівня обмеження доступу. За змістом виділяються політичні, економічні, військові, науково-технічні та інші види відомостей. За суб'єктним складом розрізняються державні, приватні та професійні інформаційні режими. За рівнем обмеження доступу встановлюються різні ступені секретності або конфіденційності [4].

Отже, розвиток інституту таємниці у праві відображає зміну підходів до регулювання інформаційних відносин, що пов'язані з розширенням цифрового середовища та збільшенням обсягів інформаційного обміну. Правова охорона таємниці виступає елементом загальної системи інформаційної безпеки, що забезпечує баланс між правом на доступ до інформації та необхідністю її захисту.

1.2. Місце таємниці в системі інформаційних правовідносин

Місце таємниці в системі інформаційних правовідносин визначається через взаємодію правових норм, що регулюють обіг інформації, встановлюють межі її відкритості та формують режими обмеженого доступу. Інформаційні правовідносини охоплюють широкий спектр суспільних зв'язків, у межах яких інформація виступає об'єктом прав, обов'язків і юридичної відповідальності. У структурі таких відносин таємниця формує особливий сегмент, пов'язаний із регламентацією прихованих або обмежених для загального доступу відомостей, що мають юридичне значення та підлягають охороні.

Функціонування інформаційних правовідносин базується на принципах відкритості інформації та одночасного встановлення правових обмежень щодо окремих її видів. У межах цієї системи таємниця виступає механізмом балансування між правом на інформацію та необхідністю захисту приватних, державних або корпоративних інтересів. Регулювання інформаційного обміну

передбачає встановлення правового режиму, що визначає порядок доступу до відомостей, умови їх використання та відповідальність за порушення встановлених правил.

Правова природа таємниці у системі інформаційних правовідносин полягає у закріпленні спеціального статусу інформації, яка вилучається з загального режиму вільного доступу. Формування такого статусу відбувається через норми законодавства або через волевиявлення суб'єктів правовідносин у межах, визначених правом [5, с.98-99]. Інформація, що набуває ознак таємниці, стає об'єктом посиленого правового захисту, що охоплює організаційні, технічні та юридичні механізми.

Структурне місце таємниці у правовій системі визначається її зв'язком з інститутами інформаційного права, цивільного права, адміністративного та кримінального права. Інформаційні правовідносини охоплюють як публічно-правові, так і приватно-правові елементи, у межах яких таємниця виступає інструментом правового регулювання інформаційного обігу. Публічно-правовий аспект пов'язаний із охороною державної інформації, приватно-правовий — із захистом комерційних, професійних та особистих відомостей.

У межах інформаційних правовідносин таємниця характеризується наявністю специфічного об'єкта, суб'єктів та змісту прав і обов'язків. Об'єктом виступає інформація з обмеженим доступом, що має визначений правовий режим. Суб'єктами виступають фізичні особи, юридичні особи, органи державної влади та інші учасники інформаційного обігу, які володіють, використовують або контролюють відповідні відомості. Зміст правовідносин формують права на володіння, використання та захист інформації, а також обов'язки щодо її нерозголошення.

У системі інформаційних правовідносин таємниця виконує роль правового інструменту захисту інформаційної автономії суб'єктів. Для фізичних осіб вона забезпечує охорону приватного життя, персональних даних та інших відомостей особистого характеру. Для юридичних осіб вона створює умови захисту комерційної інформації, виробничих процесів та фінансових

даних. Для держави вона забезпечує збереження відомостей, що стосуються національної безпеки, оборони та управління [6, с.7-8].

Таким чином, інформаційні правовідносини у сфері таємниці виступають складовою частиною правового механізму регулювання інформаційного суспільства. Формування ефективної системи охорони інформації пов'язане з удосконаленням правових інститутів, що визначають статус інформації, права суб'єктів та порядок їх реалізації.

1.3. Нормативно-правове регулювання охорони таємниці в Україні

Нормативно-правове регулювання охорони таємниці в Україні сформоване як багаторівнева система правових актів, що охоплює конституційні положення, спеціальні закони, кодекси та підзаконні нормативні документи. Регулювання спрямоване на визначення правового режиму інформації з обмеженим доступом, встановлення порядку її захисту, визначення повноважень державних органів і закріплення відповідальності за порушення встановлених правил. У межах правової системи України охорона таємниці інтегрована в загальну структуру інформаційного права та пов'язана з реалізацією гарантій інформаційної безпеки, захистом приватних інтересів і забезпеченням функціонування державних інституцій.

Конституційні засади охорони таємниці закріплені у Конституції України [7]. Конституційні норми визначають право на невтручання в особисте і сімейне життя, гарантії захисту інформації про особу, заборону збирання, зберігання та поширення конфіденційних відомостей без передбачених законом підстав. У структурі конституційного регулювання закріплено принцип обмеження доступу до інформації у випадках, коли її поширення може вплинути на права людини, інтереси суспільства або держави. Конституційні

положення формують базу для подальшого розвитку спеціального законодавства у сфері охорони інформації з обмеженим доступом.

Спеціальне законодавство у сфері охорони державної таємниці визначене Законом України «Про державну таємницю» [8]. Норми цього акта встановлюють категорії інформації, що підлягає віднесенню до державної таємниці, визначають ступені секретності, порядок засекречування і розсекречування відомостей, а також регламентують доступ до таких даних. У межах цього закону закріплено систему органів, уповноважених на здійснення контролю у сфері охорони державної таємниці, визначено вимоги до режиму секретності у державних органах, установах і організаціях. Закон визначає юридичну відповідальність за порушення правил поводження з секретною інформацією.

Адміністративно-правове регулювання охорони таємниці охоплюється положеннями Кодексу України про адміністративні правопорушення [9]. Норми кодексу передбачають відповідальність за порушення встановленого порядку доступу до інформації, недодержання режиму секретності, неправомірне використання відомостей з обмеженим доступом. Адміністративно-правові санкції застосовуються до посадових осіб і інших суб'єктів у разі порушення встановлених процедур обробки інформації.

Кримінально-правовий аспект регулювання закріплений у Кримінальному кодексі України [10]. Кримінально-правові норми визначають склад злочинів, пов'язаних із розголошенням державної таємниці, незаконним доступом до інформаційних систем, порушенням режиму конфіденційності. Кримінальна відповідальність передбачена за дії, що спричиняють розкриття відомостей, які становлять охоронювану законом таємницю, а також за створення умов для неправомірного доступу до таких даних.

Закон України «Про інформацію» [11] визначає загальні засади інформаційних відносин, класифікацію інформації за режимом доступу, порядок її поширення та захисту. Норми закону закріплюють поділ інформації на відкриту та з обмеженим доступом, встановлюють правові підстави для

віднесення відомостей до категорії конфіденційних, службових або секретних. Закон формує загальну рамку для регулювання різних видів таємниці у правовій системі.

Регулювання доступу до публічної інформації здійснюється відповідно до Закону України «Про доступ до публічної інформації» [12]. Положення акта визначають порядок реалізації права на доступ до інформації, що перебуває у володінні суб'єктів владних повноважень, а також встановлюють винятки щодо інформації з обмеженим доступом. Закон регламентує процедури запитів, строки надання відповідей і підстави для відмови у наданні інформації, що становить таємницю.

Правове регулювання у сфері національної безпеки закріплено у Законі України «Про національну безпеку України» [13]. Норми цього закону визначають систему забезпечення національної безпеки, у межах якої охорона інформації з обмеженим доступом розглядається як складова діяльності державних органів. Закон встановлює принципи функціонування сектору безпеки і оборони, що включають захист державної інформації від несанкціонованого доступу.

Закон України «Про Службу безпеки України» [14] визначає повноваження спеціального органу державної влади у сфері захисту державної таємниці та інформаційної безпеки. Служба безпеки України здійснює контроль за дотриманням режиму секретності, бере участь у захисті інформаційних ресурсів держави, проводить заходи щодо запобігання витоку відомостей з обмеженим доступом.

Регулювання захисту інформації в інформаційно-телекомунікаційних системах встановлено Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» [15]. Положення акта визначають вимоги до створення, експлуатації та захисту інформаційних систем, у яких обробляються дані з обмеженим доступом. Закон встановлює порядок впровадження технічних і організаційних заходів захисту інформації, що забезпечують її цілісність і конфіденційність.

Правовий статус державних службовців у контексті охорони таємниці регламентується Законом України «Про державну службу» [16]. Закон визначає обов'язки щодо нерозголошення інформації, отриманої під час виконання службових повноважень, встановлює вимоги до дотримання режиму доступу до службових відомостей і передбачає відповідальність за порушення цих обов'язків.

Підзаконне регулювання режиму секретності встановлено постановами Кабінету Міністрів України «Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях» [17]. Зазначені акти визначають порядок організації режиму секретності, правила роботи з документами, що містять державну таємницю, порядок допуску осіб до секретної інформації, вимоги до обліку та зберігання матеріалів.

Постанова Кабінету Міністрів України «Про затвердження Положення про порядок надання допуску до державної таємниці» [18] визначає процедуру оформлення допуску до державної таємниці, умови перевірки осіб, критерії надання або обмеження доступу до секретної інформації. Регламентація допуску формує систему індивідуального доступу до відомостей, що становлять державну таємницю.

Отже, нормативно-правове регулювання охорони таємниці в Україні охоплює комплекс взаємопов'язаних актів, що формують цілісну систему захисту інформації з обмеженим доступом. Узгодженість між конституційними положеннями, законами та підзаконними актами забезпечує функціонування правового режиму таємниці у різних сферах суспільних відносин, включаючи державне управління, економічну діяльність, професійну сферу та інформаційні технології.

РОЗДІЛ 2

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ОКРЕМИХ ВИДІВ ТАЄМНИЦІ В УКРАЇНІ

2.1. Кримінально-правова охорона державної таємниці

Кримінально-правова охорона державної таємниці в Україні становить складову системи забезпечення національної безпеки, інформаційної безпеки та стабільності функціонування державних інституцій. Правове регулювання у цій сфері спрямоване на встановлення відповідальності за протиправні дії, пов'язані з незаконним отриманням, використанням, передачею або розголошенням відомостей, що становлять державну таємницю [19, с.102-104]. Кримінально-правові норми визначають межі допустимої поведінки щодо інформації з обмеженим доступом та формують систему правових гарантій захисту секретних відомостей.

Правова природа державної таємниці пов'язана з існуванням інформації, поширення якої здатне вплинути на обороноздатність держави, зовнішньополітичну діяльність, економічну безпеку, функціонування правоохоронних органів або систему державного управління. Відомості, що становлять державну таємницю, підлягають охороні через спеціальний режим доступу, встановлений законодавством. Кримінально-правовий механізм виступає інструментом примусового забезпечення дотримання цього режиму.

Кримінально-правова охорона державної таємниці базується на положеннях Кримінального кодексу України, Закону України «Про державну таємницю», законодавства у сфері національної безпеки та інших нормативних актів, що регулюють режим секретності. У межах правової системи кримінальна відповідальність застосовується у випадках, коли порушення встановленого порядку поводження з секретною інформацією створює суспільно небезпечні наслідки або загрозу їх виникнення.

Особливість кримінально-правового захисту державної таємниці полягає у поєднанні превентивної та охоронної функцій. Превентивний аспект спрямований на запобігання протиправним діям через встановлення заборон і санкцій. Охоронний аспект пов'язаний із реагуванням держави на факти розголошення або незаконного використання секретної інформації шляхом застосування кримінального покарання.

Система злочинів у сфері охорони державної таємниці охоплює діяння, пов'язані з державною зрадою, шпигунством, розголошенням державної таємниці, втратою документів або матеріальних носіїв секретної інформації, незаконним збиранням або передачею відомостей з обмеженим доступом. Кожен із цих складів злочину має специфічні ознаки, пов'язані з характером інформації, способом вчинення діяння та суб'єктним складом.

Державна зрада займає особливе місце у системі злочинів проти державної таємниці. Зміст цього злочину пов'язаний із переходом на бік іноземної держави, наданням допомоги іноземним організаціям або представникам у проведенні підривної діяльності проти України. Передача державної таємниці іноземним суб'єктам виступає однією з форм реалізації такого діяння. Кримінально-правова кваліфікація залежить від характеру дій, суб'єктивної сторони та наявності шкоди державним інтересам.

Шпигунство характеризується незаконним збиранням або передачею інформації, що становить державну таємницю, на користь іноземної держави чи організації. Особливість цього злочину полягає у спрямованості дій на отримання секретної інформації шляхом використання прихованих методів, технічних засобів або вербування осіб, які мають доступ до секретних відомостей [20, с.96-97]. У межах кримінального законодавства шпигунство розглядається як посягання на інформаційну безпеку та державний суверенітет.

Розголошення державної таємниці охоплює випадки повідомлення секретних відомостей особам, які не мають відповідного допуску або права доступу. Форми розголошення можуть бути усними, письмовими, електронними або пов'язаними з порушенням правил зберігання інформації.

Суспільна небезпечність такого діяння визначається характером відомостей, наслідками поширення та обсягом шкоди державним інтересам.

Втрата документів або матеріальних носіїв інформації, що містять державну таємницю, становить окремий склад злочину. У цьому випадку кримінальна відповідальність пов'язана з недотриманням встановлених правил поводження із секретними матеріалами. Втрата документів може створювати умови для доступу сторонніх осіб до секретної інформації та спричиняти ризики для державної безпеки.

Кримінально-правова охорона державної таємниці поширюється на інформацію, яка пройшла процедуру засекречування відповідно до законодавства. Для настання кримінальної відповідальності необхідним є встановлення факту, що відомості дійсно належать до категорії державної таємниці та мають відповідний ступінь секретності. Юридичне значення у таких справах має наявність грифу секретності, а також дотримання процедури віднесення інформації до категорії секретної.

Суб'єктами злочинів у сфері охорони державної таємниці виступають фізичні осудні особи, які досягли встановленого законом віку кримінальної відповідальності. У низці випадків обов'язковою ознакою суб'єкта виступає наявність спеціального статусу, пов'язаного з доступом до державної таємниці [21, с.88-89]. До таких осіб належать державні службовці, військовослужбовці, працівники правоохоронних органів, представники підприємств та установ, які виконують роботи, пов'язані з державною таємницею.

Суб'єктивна сторона злочинів проти державної таємниці характеризується умисною або необережною формою вини залежно від конкретного складу злочину. Державна зрада та шпигунство вчиняються умисно, оскільки передбачають усвідомлення характеру інформації та спрямованість дій на передачу відомостей іноземним суб'єктам. Втрата документів або порушення правил поводження із секретною інформацією можуть бути пов'язані з необережною формою вини.

Кримінально-правова охорона державної таємниці пов'язана з діяльністю правоохоронних органів та спеціальних служб, уповноважених на виявлення, припинення та розслідування відповідних злочинів. Особливе місце у цій системі займає Служба безпеки України, яка здійснює контррозвідальну діяльність, контроль за режимом секретності та заходи протидії інформаційним загрозам.

Розслідування злочинів, пов'язаних із державною таємницею, має специфічний процесуальний характер. Кримінальне провадження у таких справах супроводжується обмеженням доступу до матеріалів, використанням спеціального порядку роботи з доказами та дотриманням режиму секретності під час судового розгляду. Органи досудового розслідування зобов'язані забезпечувати захист секретної інформації у процесі проведення слідчих дій.

Технічний розвиток інформаційного середовища вплинув на трансформацію механізмів кримінально-правової охорони державної таємниці. Поширення електронного документообігу, використання цифрових мереж та автоматизованих систем обробки даних створили нові способи незаконного доступу до секретної інформації. У зв'язку з цим кримінально-правове регулювання охоплює діяння, пов'язані з втручанням у роботу інформаційно-комунікаційних систем, несанкціонованим копіюванням електронних даних та використанням шкідливого програмного забезпечення.

Міжнародний аспект кримінально-правової охорони державної таємниці пов'язаний із співробітництвом держав у сфері протидії шпигунству, кіберзлочинності та незаконному обігу інформації. Участь України у міжнародних договорах у сфері безпеки формує додаткові механізми взаємодії між правоохоронними органами різних держав щодо обміну інформацією та проведення спільних заходів [22, с.86-87].

Кримінально-правовий захист державної таємниці має зв'язок із забезпеченням інформаційної безпеки держави. Захист секретної інформації спрямований на збереження стабільності функціонування органів державної

влади, оборонного сектору, системи правоохоронних органів та інших сфер, пов'язаних із реалізацією державної політики.

Правове значення кримінальної відповідальності у сфері охорони державної таємниці полягає у формуванні механізму примусового забезпечення режиму секретності. Кримінальне покарання виступає реакцією держави на суспільно небезпечні діяння, що посягають на захищену інформацію та створюють загрозу для державних інтересів.

Таким чином, кримінально-правова охорона державної таємниці в Україні охоплює комплекс правових норм, організаційних заходів та діяльність спеціально уповноважених органів, спрямованих на забезпечення захисту інформації з обмеженим доступом. Система правового регулювання у цій сфері формується з урахуванням сучасних інформаційних загроз, розвитку цифрових технологій та змін у сфері національної безпеки.

2.2. Кримінальна відповідальність за порушення таємниці приватного життя, листування, телефонних розмов та іншої кореспонденції

Кримінальна відповідальність за порушення таємниці приватного життя, листування, телефонних розмов та іншої кореспонденції становить складову системи захисту конституційних прав людини та громадянина. Охорона приватної сфери особи пов'язана із забезпеченням недоторканності інформації, що стосується особистого життя, сімейних відносин, комунікацій та інших відомостей індивідуального характеру. Правове регулювання у цій сфері ґрунтується на конституційних гарантіях, положеннях кримінального законодавства та міжнародних стандартах у сфері прав людини [23, с.23-24].

Конституція України закріплює право кожної особи на невтручання в особисте і сімейне життя, гарантує таємницю листування, телефонних розмов,

телеграфної та іншої кореспонденції. Обмеження таких прав допускається виключно у випадках, визначених законом, на підставі судового рішення та у межах, пов'язаних із забезпеченням кримінального провадження або національної безпеки. Кримінально-правовий механізм охорони приватного життя спрямований на забезпечення реалізації зазначених конституційних гарантій.

Поняття приватного життя охоплює сферу особистих відносин людини, інформацію про сімейний стан, стан здоров'я, місце проживання, особисті контакти, звички, погляди та інші відомості, що не підлягають вільному поширенню без згоди особи. У межах кримінально-правової охорони захист поширюється на будь-яку інформацію, що має приватний характер і не призначена для відкритого доступу.

Таємниця листування, телефонних розмов та іншої кореспонденції охоплює інформацію, що передається через поштові, телекомунікаційні, електронні та інші засоби зв'язку. Правовий режим такої інформації передбачає обмеження доступу до змісту повідомлень, даних про відправника та отримувача, часу та способу комунікації. Незаконне отримання, поширення або використання таких відомостей визнається порушенням прав людини та підставою для кримінальної відповідальності.

Кримінальний кодекс України встановлює відповідальність за порушення недоторканності приватного життя, незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди. Кримінально караними визнаються дії, пов'язані з втручанням у сферу особистих комунікацій, прослуховуванням телефонних розмов, перехопленням електронної кореспонденції, незаконним доступом до особистих повідомлень або розголошенням отриманих відомостей [24, с.113-114].

Правова природа злочинів проти таємниці приватного життя полягає у посяганні на інформаційну автономію особи. Захист приватної інформації спрямований на забезпечення свободи спілкування, недоторканності особистих зв'язків та охорону внутрішньої сфери життя людини від стороннього

втручання. Порушення режиму конфіденційності створює ризики неправомірного використання інформації, втручання у сімейні відносини, психологічного тиску або дискредитації особи.

Об'єктом кримінально-правової охорони виступають суспільні відносини, пов'язані із забезпеченням права на приватність та таємницю комунікацій. Предметом злочину можуть бути листи, електронні повідомлення, записи телефонних розмов, інформація з електронних пристроїв, особисті документи та інші носії конфіденційної інформації.

Незаконне збирання конфіденційної інформації про особу охоплює отримання відомостей без правових підстав або без згоди особи. Такі дії можуть здійснюватися шляхом прихованого спостереження, використання технічних засобів, доступу до електронних систем або шляхом отримання інформації від третіх осіб. Особливість кримінально-правової оцінки полягає у визначенні незаконності способу отримання інформації.

Зберігання конфіденційної інформації без належних підстав також підпадає під кримінально-правову заборону у випадках, коли така інформація отримана незаконним шляхом або використовується всупереч вимогам закону. Використання відомостей про особу без її згоди може проявлятися у передачі інформації третім особам, публікації у засобах масової інформації, використанні у господарській діяльності або поширенні через мережу Інтернет.

Поширення конфіденційної інформації про особу становить одну з найбільш поширених форм порушення права на приватність. У сучасному інформаційному середовищі розповсюдження особистих даних через цифрові платформи створює значні ризики для захисту приватного життя. Публікація особистого листування, фотографій, аудіозаписів або інших матеріалів без згоди особи може спричиняти юридичні наслідки у вигляді кримінальної відповідальності [25, с.338-339].

Порушення таємниці телефонних розмов охоплює незаконне прослуховування, запис або перехоплення комунікацій без передбачених законом підстав. Використання технічних пристроїв для прихованого

отримання інформації про зміст розмов визнається втручанням у приватне життя. Кримінально-правова оцінка залежить від способу вчинення діяння, характеру отриманої інформації та наявності умислу.

Електронна кореспонденція у сучасних умовах становить окремий об'єкт правового захисту. Використання електронної пошти, месенджерів, соціальних мереж та інших цифрових платформ призвело до розширення форм комунікації, що потребують правової охорони. Незаконний доступ до електронних повідомлень, копіювання даних або їх поширення визнаються порушенням таємниці кореспонденції.

Кримінальна відповідальність у сфері охорони приватного життя поширюється на випадки незаконного використання спеціальних технічних засобів отримання інформації. До таких засобів належать пристрої для прихованого аудіо- або відеозапису, програмне забезпечення для перехоплення електронних повідомлень, засоби дистанційного доступу до цифрових пристроїв. Використання подібних технологій без правових підстав визнається протиправним.

Суб'єктом злочинів проти таємниці приватного життя виступає фізична осудна особа, яка досягла встановленого законом віку кримінальної відповідальності. У певних випадках відповідальність може наставати для службових осіб, які використовують службове становище для незаконного отримання або поширення конфіденційної інформації.

Суб'єктивна сторона таких злочинів характеризується переважно умисною формою вини. Особа усвідомлює конфіденційний характер інформації, розуміє незаконність своїх дій та передбачає наслідки втручання у приватне життя [26, с.655-656]. Мотиви вчинення злочину можуть бути різними, включаючи корисливі інтереси, помсту, отримання переваг або поширення інформації з метою впливу на потерпілого.

Особливості кримінального провадження у справах про порушення таємниці приватного життя пов'язані з необхідністю забезпечення конфіденційності під час розслідування. Органи досудового розслідування та

суди зобов'язані вживати заходів щодо недопущення повторного розголошення інформації, яка стала предметом кримінального провадження. Процесуальні дії здійснюються з урахуванням права потерпілої особи на захист приватного життя.

Правове регулювання у сфері охорони таємниці приватного життя має зв'язок із міжнародними стандартами прав людини. Європейська конвенція з прав людини закріплює право на повагу до приватного і сімейного життя, житла та кореспонденції. Практика Європейського суду з прав людини формує підходи до оцінки допустимості втручання держави у сферу приватних комунікацій.

Розвиток цифрових технологій спричинив ускладнення механізмів кримінально-правового захисту приватності. Використання хмарних сервісів, мобільних застосунків, систем відеоспостереження та електронних баз даних створює нові форми ризиків для конфіденційності інформації. Кримінально-правове регулювання поступово адаптується до змін інформаційного середовища через розширення правових механізмів захисту електронної інформації.

Отже, кримінальна відповідальність за порушення таємниці приватного життя, листування, телефонних розмов та іншої кореспонденції спрямована на забезпечення недоторканності особистої сфери людини та охорону конфіденційної інформації від незаконного втручання. Система кримінально-правового захисту у цій сфері охоплює комплекс правових норм, діяльність правоохоронних органів і процесуальні механізми, пов'язані з виявленням, припиненням та розслідуванням відповідних правопорушень.

2.3. Охорона комерційної, банківської, професійної та службової таємниці засобами кримінального права

Охорона комерційної, банківської, професійної та службової таємниці засобами кримінального права пов'язана із забезпеченням стабільності інформаційних відносин у сфері економічної діяльності, функціонування фінансових установ, виконання професійних обов'язків та здійснення державного управління. Інформація з обмеженим доступом у зазначених сферах має правовий режим, що передбачає обов'язок нерозголошення, встановлення кола уповноважених осіб та застосування юридичної відповідальності за неправомірне використання або поширення відомостей. Кримінально-правова охорона виступає елементом механізму забезпечення конфіденційності інформації та захисту інтересів фізичних осіб, юридичних осіб і держави.

Комерційна таємниця становить сукупність відомостей, пов'язаних із господарською діяльністю суб'єкта підприємництва, які мають економічну цінність у зв'язку з обмеженим доступом до них. До категорії комерційної таємниці відносяться виробничі технології, фінансові показники, відомості про клієнтів, бізнес-плани, умови договорів, маркетингові стратегії та інші дані, використання яких впливає на конкурентне становище підприємства. Правовий режим такої інформації формується на підставі законодавства та внутрішніх документів суб'єкта господарювання.

Кримінально-правова охорона комерційної таємниці спрямована на запобігання незаконному збиранню, використанню або розголошенню інформації, що становить економічну цінність для підприємства. Незаконне отримання комерційної інформації може здійснюватися шляхом викрадення документів, втручання в інформаційні системи, підкупу працівників або використання технічних засобів доступу до даних [27, с.61-62]. Подібні дії створюють ризики порушення господарської діяльності, втрати конкурентних переваг та спричинення матеріальних збитків.

Кримінальний кодекс України передбачає відповідальність за незаконне збирання відомостей, що становлять комерційну таємницю, а також за розголошення такої інформації без згоди власника. Юридична оцінка діяння

залежить від способу отримання інформації, наявності умислу, обсягу заподіяної шкоди та характеру використання відомостей. Розголошення комерційної інформації працівниками підприємств або іншими особами, яким вона стала відома у зв'язку з виконанням службових чи професійних обов'язків, визнається підставою для кримінальної відповідальності у випадках, передбачених законом.

Банківська таємниця охоплює інформацію про рахунки, фінансові операції, майновий стан клієнтів банківських установ, а також інші відомості, отримані під час банківського обслуговування. Правовий режим банківської таємниці спрямований на забезпечення конфіденційності фінансової інформації та підтримання стабільності банківської системи. Доступ до таких відомостей обмежується колом осіб, визначених законодавством.

Кримінально-правова охорона банківської таємниці пов'язана із захистом інформації від незаконного розголошення, копіювання або використання. Порушення режиму конфіденційності може проявлятися у передачі відомостей стороннім особам, використанні інформації у корисливих цілях або поширенні даних про клієнтів банківських установ без законних підстав. Суспільна небезпечність подібних діянь полягає у створенні ризиків фінансових втрат, порушенні прав клієнтів та підриві довіри до банківської системи.

Кримінальна відповідальність у сфері банківської таємниці настає у випадках незаконного розголошення або використання інформації, отриманої під час професійної діяльності. Суб'єктами відповідних злочинів можуть виступати працівники банків, посадові особи фінансових установ, державні службовці або інші особи, які отримали доступ до конфіденційних відомостей у зв'язку з виконанням професійних функцій [28, с.77-78].

Професійна таємниця охоплює інформацію, що стала відомою особі у процесі здійснення професійної діяльності та підлягає нерозголошенню відповідно до законодавства або професійних стандартів. До цієї категорії відносяться адвокатська, медична, нотаріальна, аудиторська та інші види

професійної таємниці. Охорона таких відомостей пов'язана із забезпеченням довірчих відносин між особою та представником відповідної професії.

Адвокатська таємниця включає інформацію про клієнта, зміст консультацій, документи, отримані адвокатом під час надання правової допомоги. Кримінально-правовий захист у цій сфері спрямований на забезпечення конфіденційності правничої діяльності та гарантування права особи на професійну правову допомогу. Незаконне втручання у сферу адвокатської діяльності, отримання або поширення інформації про клієнта без законних підстав може розглядатися як кримінально каране діяння.

Медична таємниця охоплює інформацію про стан здоров'я, результати медичних обстежень, діагнози та інші відомості, отримані під час надання медичної допомоги. Кримінально-правова охорона медичної інформації пов'язана із забезпеченням права особи на конфіденційність відомостей про здоров'я. Розголошення медичної таємниці без згоди пацієнта або без передбачених законом підстав визнається порушенням права на приватне життя.

Нотаріальна таємниця стосується інформації, отриманої нотаріусом під час вчинення нотаріальних дій. Правовий режим охоплює документи, відомості про учасників правочинів, зміст юридичних дій та інші дані, що стали відомими у процесі професійної діяльності. Порушення режиму конфіденційності у цій сфері створює підстави для застосування юридичної відповідальності.

Службова таємниця охоплює інформацію, що формується або використовується у процесі діяльності державних органів, органів місцевого самоврядування, підприємств та установ і не підлягає відкритому поширенню. До службової інформації відносяться внутрішні документи, службове листування, аналітичні матеріали, організаційні рішення та інші відомості, доступ до яких обмежується у зв'язку з характером службової діяльності.

Кримінально-правова охорона службової таємниці спрямована на забезпечення належного функціонування органів влади та інших установ. Незаконне розголошення службової інформації може впливати на діяльність

державних органів, створювати ризики для безпеки інформаційних систем або порушувати права громадян [29, с.356-357]. Особливість службової таємниці полягає у її зв'язку з виконанням службових повноважень та адміністративних функцій.

Об'єктом кримінально-правової охорони у сфері комерційної, банківської, професійної та службової таємниці виступають суспільні відносини, пов'язані із забезпеченням конфіденційності інформації та захистом прав суб'єктів інформаційних відносин. Предметом злочину можуть бути документи, електронні дані, записи, бази даних, повідомлення та інші носії інформації з обмеженим доступом.

Суб'єктами відповідних злочинів виступають фізичні осудні особи, які досягли встановленого законом віку кримінальної відповідальності. У низці випадків обов'язковою ознакою суб'єкта є спеціальний статус особи, пов'язаний із виконанням професійних або службових обов'язків. До таких осіб належать працівники банківських установ, медичні працівники, адвокати, нотаріуси, державні службовці, працівники підприємств та інші особи, яким інформація стала відома у зв'язку з професійною діяльністю.

Суб'єктивна сторона злочинів у сфері охорони таємниці характеризується переважно умисною формою вини. Особа усвідомлює конфіденційний характер інформації, розуміє обмеження щодо її поширення та передбачає наслідки своїх дій. Мотиви вчинення злочинів можуть бути пов'язані з корисливими інтересами, конкурентною боротьбою, помстою, отриманням вигоди або використанням інформації в інтересах третіх осіб.

Кримінально-правова охорона комерційної, банківської, професійної та службової таємниці пов'язана з діяльністю правоохоронних органів, судових установ та спеціальних органів контролю. Розслідування відповідних злочинів супроводжується необхідністю встановлення факту конфіденційності інформації, наявності правового режиму доступу та обставин незаконного отримання або поширення відомостей.

Таким чином, система кримінально-правового захисту інформації з обмеженим доступом охоплює комплекс правових механізмів, спрямованих на забезпечення конфіденційності у різних сферах суспільних відносин. Правове регулювання у цій сфері формується з урахуванням розвитку інформаційних технологій, зміни форм професійної діяльності та ускладнення інформаційного обігу у сучасному суспільстві.

РОЗДІЛ 3

ПРОБЛЕМИ ТА НАПЯМИ УДОСКОНАЛЕННЯ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ТАЄМНИЦІ В УКРАЇНІ

3.1. Проблеми кваліфікації кримінальних правопорушень, пов'язаних із розголошенням таємниці

Проблеми кваліфікації кримінальних правопорушень, пов'язаних із розголошенням таємниці, посідають значне місце у сфері кримінально-правового регулювання інформаційних відносин. У процесі правозастосування виникають труднощі, пов'язані з визначенням предмета злочину, встановленням правового режиму інформації, розмежуванням суміжних складів кримінальних правопорушень та оцінкою наслідків протиправних дій. Інформація з обмеженим доступом охоплює різні види відомостей, серед яких державна, комерційна, банківська, професійна, службова та інші форми таємниці. Кожна категорія має окремі правові ознаки, що впливають на особливості кримінально-правової кваліфікації.

Однією з проблем у сфері кваліфікації виступає встановлення факту належності інформації до категорії таємниці. Для притягнення особи до кримінальної відповідальності необхідним є підтвердження існування правового режиму обмеженого доступу до відповідних відомостей. Відомості повинні бути віднесені до певного виду таємниці на підставі закону, підзаконного нормативного акта, внутрішніх документів підприємства або професійних правил [30, с.39-40]. Відсутність належного оформлення режиму конфіденційності ускладнює визначення предмета кримінального правопорушення.

Складність правозастосування виникає у випадках, коли інформація частково містить відомості з обмеженим доступом або одночасно охоплює декілька правових режимів. Наприклад, документи можуть поєднувати

службову інформацію з персональними даними або містити елементи комерційної таємниці й банківської інформації. У подібних ситуаціях виникає потреба у визначенні пріоритетного правового режиму та правильному застосуванні норм кримінального законодавства.

Проблеми кваліфікації стосуються розмежування кримінально караного розголошення інформації та дисциплінарного або адміністративного порушення режиму конфіденційності. Не кожне порушення правил поведінки з інформацією утворює склад кримінального правопорушення. Для кримінально-правової оцінки необхідним є встановлення суспільно небезпечного характеру діяння, наявності визначених законом ознак злочину та відповідного рівня шкоди. Відсутність істотних наслідків або незначний характер порушення можуть свідчити про необхідність застосування інших видів юридичної відповідальності.

Труднощі виникають у процесі встановлення об'єктивної сторони кримінального правопорушення. Розголошення таємниці може здійснюватися у різних формах, включаючи усне повідомлення, передачу документів, електронне копіювання даних, публікацію інформації у мережі Інтернет або надання доступу стороннім особам до інформаційних систем. У кожному випадку необхідним є встановлення способу вчинення діяння, обсягу поширених відомостей та факту доступу сторонніх осіб до конфіденційної інформації [31, с.387-388].

Особливе значення у кваліфікації кримінальних правопорушень має встановлення суб'єкта злочину. У низці складів кримінальних правопорушень суб'єкт є спеціальним, оскільки відповідальність настає для осіб, яким інформація була довірена або стала відома у зв'язку з професійною чи службовою діяльністю. До таких осіб належать державні службовці, працівники правоохоронних органів, адвокати, медичні працівники, банківські працівники та інші суб'єкти, які мають законний доступ до конфіденційної інформації. Встановлення зв'язку між професійними обов'язками особи та

фактом доступу до інформації має визначальне значення для правильної кваліфікації.

Проблеми виникають у випадках, коли доступ до інформації був отриманий незаконно або випадково. Якщо особа не мала законного права доступу до інформації, постає питання щодо кваліфікації дій як незаконного отримання інформації, втручання у роботу інформаційних систем або іншого суміжного кримінального правопорушення. Розмежування таких складів потребує аналізу способу отримання інформації та подальших дій із нею.

Складність кримінально-правової оцінки пов'язана з визначенням форми вини. Розголошення таємниці може бути умисним або необережним. Умисна форма вини передбачає усвідомлення особою конфіденційного характеру інформації та бажання або свідоме допущення її поширення. Необережна форма вини пов'язана з порушенням правил поведінки з інформацією через недбалість або несумлінне ставлення до службових обов'язків. Встановлення психічного ставлення особи до вчиненого діяння має значення для визначення правильної правової кваліфікації.

Проблемним аспектом виступає оцінка наслідків розголошення інформації. У низці складів кримінальних правопорушень обов'язковою ознакою є настання шкоди або створення загрози її виникнення. Визначення обсягу шкоди у сфері інформаційних правовідносин ускладнюється нематеріальним характером інформації [32, с.92-94]. Наслідки можуть проявлятися у фінансових збитках, порушенні діяльності державних органів, втраті ділової репутації, втручанні у приватне життя або створенні загроз для національної безпеки.

Розвиток цифрових технологій спричинив появу нових проблем у сфері кваліфікації кримінальних правопорушень, пов'язаних із розголошенням таємниці. Використання електронних засобів комунікації, хмарних сервісів, цифрових баз даних та автоматизованих інформаційних систем створило нові форми поширення конфіденційної інформації. Незаконне копіювання електронних файлів, пересилання інформації через мережу Інтернет або доступ

до віддалених серверів ускладнюють встановлення способу вчинення діяння та кола причетних осіб.

Складність кваліфікації виникає у випадках використання спеціальних технічних засобів отримання інформації. Прослуховування телефонних розмов, прихований аудіо- або відеозапис, використання шкідливого програмного забезпечення для доступу до інформаційних систем можуть утворювати сукупність кримінальних правопорушень. У таких ситуаціях необхідним є правильне розмежування незаконного отримання інформації, втручання у роботу інформаційних систем та безпосереднього розголошення таємниці.

Міжнародний характер сучасних інформаційних відносин створює додаткові труднощі у процесі кваліфікації. Передача інформації через міжнародні електронні мережі, використання іноземних серверів та участь іноземних суб'єктів у поширенні конфіденційних відомостей ускладнюють визначення юрисдикції, порядку розслідування та застосування кримінального законодавства. Транснаціональний характер інформаційних правопорушень потребує взаємодії між правоохоронними органами різних держав.

Отже, проблеми кваліфікації кримінальних правопорушень, пов'язаних із розголошенням таємниці, пов'язані з розвитком інформаційних технологій, ускладненням інформаційних відносин та різноманітністю форм конфіденційної інформації. Правозастосовна практика у цій сфері потребує чіткого визначення правового режиму інформації, правильного розмежування суміжних складів кримінальних правопорушень та врахування особливостей сучасного цифрового середовища.

3.2. Зарубіжний досвід кримінально-правової охорони таємниці

Зарубіжний досвід кримінально-правової охорони таємниці формується під впливом особливостей правових систем, розвитку інформаційних

технологій, підходів до забезпечення прав людини та рівня державного контролю у сфері інформаційних відносин. У більшості держав правове регулювання охорони таємниці охоплює захист державної, комерційної, банківської, професійної та приватної інформації. Кримінально-правові механізми спрямовані на встановлення відповідальності за незаконне отримання, використання або розголошення відомостей з обмеженим доступом.

Правові системи держав Європейського Союзу базуються на поєднанні національного законодавства та загальноєвропейських стандартів захисту інформації. Особливе місце у сфері правового регулювання посідає захист персональних даних і приватного життя. Законодавство багатьох європейських держав передбачає кримінальну відповідальність за незаконне збирання або поширення конфіденційної інформації, втручання у приватні комунікації та порушення режиму професійної таємниці.

У Німеччині кримінально-правова охорона таємниці регламентується положеннями Кримінального кодексу Федеративної Республіки Німеччина та спеціальними законами у сфері захисту даних і державної безпеки. Законодавство передбачає відповідальність за порушення таємниці листування, незаконне використання персональних даних, розголошення професійної та комерційної інформації. Окремі норми стосуються відповідальності працівників державних органів та осіб, які мають доступ до конфіденційних відомостей у зв'язку з професійною діяльністю [33, с.13-14].

Французьке кримінальне законодавство охоплює захист приватного життя, професійної таємниці та державної інформації. Кримінальний кодекс Франції встановлює відповідальність за незаконне прослуховування телефонних розмов, втручання у приватне життя, порушення таємниці кореспонденції та незаконне поширення інформації про особу. Значна увага приділяється захисту медичної, адвокатської та банківської таємниці.

Правова система Великої Британії характеризується поєднанням законодавчих норм і судового прецеденту. Охорона державної таємниці здійснюється відповідно до спеціальних актів, що встановлюють

відповідальність за розголошення секретної інформації державними службовцями, військовослужбовцями та іншими особами, які мають доступ до відомостей з обмеженим доступом. Законодавство Великої Британії охоплює кримінальну відповідальність за незаконне використання інформації у сфері національної безпеки та оборони.

У Сполучених Штатах Америки кримінально-правова охорона таємниці пов'язана із захистом державної безпеки, економічних інтересів і прав громадян на приватність. Федеральне законодавство встановлює відповідальність за шпигунство, незаконне розголошення державної інформації, порушення банківської таємниці та незаконний доступ до електронних комунікацій. Окреме місце займає регулювання кіберзлочинності, пов'язаної з викраденням конфіденційної інформації через інформаційні системи та комп'ютерні мережі.

Американське законодавство у сфері захисту комерційної таємниці передбачає кримінальну відповідальність за економічне шпигунство, незаконне отримання технологічної інформації та використання комерційних секретів у конкурентній діяльності. Значна увага приділяється охороні інтелектуальної власності та інформації, пов'язаної з інноваційною діяльністю підприємств.

У Японії кримінально-правова охорона таємниці формується з урахуванням розвитку технологічного сектору та високого рівня цифровізації суспільства. Законодавство передбачає відповідальність за незаконне розголошення державної інформації, комерційних секретів і персональних даних. Окремі норми стосуються захисту інформації у сфері промислового виробництва, електронних комунікацій та діяльності фінансових установ.

Правова система Канади поєднує кримінально-правові та адміністративні механізми захисту інформації з обмеженим доступом. Кримінальне законодавство охоплює відповідальність за порушення таємниці приватного життя, незаконний доступ до інформаційних систем, використання спеціальних технічних засобів для отримання конфіденційної інформації та розголошення державних секретів. Значна увага приділяється захисту персональних даних у цифровому середовищі.

У міжнародній практиці простежується тенденція до розширення кримінально-правової охорони електронної інформації та цифрових комунікацій. Використання хмарних технологій, електронного документообігу, соціальних мереж та мобільних застосунків спричинило появу нових форм інформаційних правопорушень. У багатьох державах кримінальне законодавство адаптується до сучасних інформаційних загроз через встановлення відповідальності за кібершпигунство, несанкціонований доступ до баз даних та поширення конфіденційної інформації через цифрові мережі.

Міжнародно-правове регулювання охорони таємниці пов'язане з діяльністю міжнародних організацій та укладенням багатосторонніх угод у сфері боротьби з кіберзлочинністю та захисту інформації. Конвенція Ради Європи про кіберзлочинність визначає механізми міжнародного співробітництва у сфері протидії незаконному доступу до комп'ютерних систем, перехопленню інформації та втручанню у функціонування інформаційних ресурсів. Міжнародні стандарти формують загальні підходи до захисту інформації у цифровому середовищі [34, с.299-300].

Таким чином, кримінально-правова охорона таємниці у зарубіжних країнах спрямована на забезпечення захисту приватних, корпоративних та державних інтересів у сфері інформаційних відносин. Правові механізми у цій сфері формуються з урахуванням особливостей національних правових систем, міжнародних стандартів та сучасних викликів інформаційного суспільства.

3.3. Шляхи вдосконалення кримінального законодавства України у сфері охорони таємниці

Удосконалення кримінального законодавства України у сфері охорони таємниці пов'язане з розвитком інформаційного суспільства, зміною характеру інформаційних відносин та поширенням цифрових технологій у діяльності

державних органів, підприємств і громадян. Сучасне інформаційне середовище характеризується зростанням обсягів електронних даних, використанням автоматизованих систем обробки інформації та активним розвитком електронних комунікацій. У таких умовах кримінально-правові механізми охорони таємниці потребують адаптації до нових форм протиправної діяльності, пов'язаної з незаконним отриманням, використанням або поширенням конфіденційної інформації.

Одним із напрямів удосконалення кримінального законодавства виступає уточнення понятійного апарату у сфері охорони таємниці. У правозастосовній практиці виникають труднощі, пов'язані з розмежуванням державної, службової, комерційної, професійної та іншої інформації з обмеженим доступом. Наявність різних нормативних підходів до визначення видів таємниці створює проблеми під час кваліфікації кримінальних правопорушень. Узгодження термінології у кримінальному законодавстві та спеціальних нормативних актах сприятиме більш чіткому визначенню предмета кримінально-правової охорони.

Окремого значення набуває удосконалення кримінально-правових норм, пов'язаних із захистом електронної інформації. Використання цифрових мереж, хмарних сервісів, електронного документообігу та автоматизованих інформаційних систем спричинило появу нових способів незаконного доступу до конфіденційної інформації. Кримінальне законодавство потребує більш детального регулювання відповідальності за несанкціоноване копіювання електронних даних, втручання у функціонування інформаційних систем та поширення інформації через цифрові платформи [35, с.174-175].

Поширення кіберзлочинності впливає на необхідність посилення кримінально-правової охорони державної таємниці, комерційної інформації та персональних даних. Незаконне використання шкідливого програмного забезпечення, віддалений доступ до серверів, перехоплення електронних повідомлень та втручання у роботу комп'ютерних мереж створюють нові загрози для інформаційної безпеки. Удосконалення кримінального

законодавства у цій сфері пов'язане із закріпленням сучасних форм кримінально караних діянь та адаптацією правових механізмів до цифрового середовища.

Подальшого розвитку потребує система кримінально-правового захисту персональних даних і приватного життя. Зростання кількості електронних баз даних, використання мобільних застосунків, соціальних мереж та онлайн-платформ спричиняє збільшення ризиків незаконного поширення інформації про особу. Удосконалення законодавства може охоплювати деталізацію складів кримінальних правопорушень, пов'язаних із незаконним обігом персональних даних, використанням цифрових профілів та втручанням у приватні комунікації.

Необхідність удосконалення кримінального законодавства пов'язана з проблемами кваліфікації кримінальних правопорушень у сфері охорони таємниці. Правозастосовна практика свідчить про труднощі розмежування суміжних складів злочинів, визначення форми вини та оцінки наслідків розголошення конфіденційної інформації. Більш чітке формулювання диспозицій кримінально-правових норм сприятиме однаковому застосуванню законодавства та зменшенню кількості колізій у процесі розслідування і судового розгляду.

Удосконалення кримінального законодавства у сфері охорони таємниці пов'язане з гармонізацією українського законодавства з міжнародними стандартами та правом Європейського Союзу. Європейські підходи до захисту персональних даних, електронних комунікацій та інформаційної безпеки впливають на формування сучасних моделей правового регулювання. Імплементация міжнародних стандартів сприятиме розвитку механізмів міжнародного співробітництва у сфері боротьби з кіберзлочинністю та незаконним поширенням інформації.

Потреба у вдосконаленні законодавства пов'язана з розвитком механізмів захисту професійної таємниці. Адвокатська, медична, банківська та інші види професійної інформації потребують більш детального кримінально-правового

регулювання з урахуванням сучасних форм обробки та зберігання даних. Використання електронних реєстрів і дистанційних сервісів створює ризики несанкціонованого доступу до конфіденційної інформації, що потребує оновлення підходів до кримінально-правового захисту.

У сфері охорони державної таємниці удосконалення кримінального законодавства пов'язане із забезпеченням ефективного реагування на сучасні загрози національній безпеці. Використання цифрових технологій у сфері оборони, державного управління та функціонування критичної інфраструктури потребує посилення кримінально-правових механізмів протидії витоку секретної інформації. Особливого значення набуває захист інформаційних ресурсів у період воєнного стану та в умовах гібридних загроз.

Розвиток інформаційного суспільства впливає на необхідність удосконалення процесуальних механізмів розслідування кримінальних правопорушень, пов'язаних із розголошенням таємниці. Використання електронних доказів, цифрових носіїв інформації та результатів комп'ютерно-технічних експертиз потребує уточнення процесуальних норм щодо збирання, дослідження та оцінки доказів у кримінальному провадженні.

Значний вплив на удосконалення кримінального законодавства має розвиток міжнародного співробітництва у сфері інформаційної безпеки. Транснаціональний характер сучасних інформаційних правопорушень ускладнює діяльність правоохоронних органів та потребує координації між державами у питаннях обміну інформацією, проведення спільних розслідувань та виконання процесуальних дій за межами національної юрисдикції.

Отже, удосконалення кримінального законодавства України у сфері охорони таємниці охоплює комплекс напрямів, пов'язаних із оновленням правових норм, адаптацією до цифрового середовища, гармонізацією з міжнародними стандартами та підвищенням ефективності правозастосовної практики. Подальший розвиток правового регулювання у цій сфері пов'язаний із необхідністю врахування сучасних інформаційних загроз, трансформації

способів обробки даних та зміни характеру інформаційних відносин у суспільстві.

ВИСНОВКИ

Охорона таємниці в Україні засобами кримінального права пов'язана із забезпеченням стабільності інформаційних відносин, функціонуванням державних інституцій, захистом приватного життя людини та підтриманням належного рівня безпеки у різних сферах суспільної діяльності. Інформація з обмеженим доступом охоплює державну, комерційну, банківську, службову, професійну та інші види таємниці, що мають правове значення для держави, юридичних осіб і громадян. Кримінально-правові механізми у цій сфері спрямовані на встановлення відповідальності за незаконне отримання, використання, розголошення або поширення конфіденційних відомостей.

Державна таємниця пов'язана із захистом відомостей у сфері оборони, національної безпеки, зовнішньої політики та діяльності правоохоронних органів. Незаконне розголошення або передача секретної інформації створює ризики для суверенітету держави, обороноздатності та стабільності функціонування державних органів. Кримінальне законодавство встановлює відповідальність за шпигунство, державну зраду, розголошення державної таємниці та інші діяння, пов'язані з порушенням режиму секретності. Наявність кримінально-правових заборон формує механізм стримування протиправної поведінки у сфері захисту державної інформації.

Охорона комерційної таємниці засобами кримінального права пов'язана із забезпеченням стабільності господарської діяльності та захистом економічних інтересів суб'єктів підприємництва. Конфіденційна інформація у сфері бізнесу охоплює виробничі технології, фінансові показники, дані про клієнтів, внутрішню документацію та інші відомості, що мають економічну цінність. Незаконне використання або поширення подібної інформації може спричиняти фінансові збитки, порушення конкурентних відносин і втрату ділової репутації підприємств.

Банківська таємниця становить складову фінансової безпеки та пов'язана із захистом інформації про рахунки, операції та майновий стан клієнтів фінансових установ. Порушення конфіденційності банківської інформації впливає на права фізичних і юридичних осіб, створює ризики незаконного використання фінансових даних та підриває стабільність банківської системи. Кримінально-правові механізми охорони банківської таємниці спрямовані на запобігання незаконному доступу до фінансової інформації та її використанню у протиправних цілях.

Захист таємниці приватного життя пов'язаний із забезпеченням конституційних прав людини та охороною конфіденційної інформації про особу. Таємниця листування, телефонних розмов, електронних повідомлень і персональних даних належить до сфери приватних правовідносин. Незаконне втручання у приватне життя через прослуховування комунікацій, перехоплення електронних повідомлень або поширення особистої інформації створює загрозу порушення прав людини.

Службова таємниця пов'язана з діяльністю державних органів, органів місцевого самоврядування, підприємств та установ. Інформація службового характеру охоплює внутрішню документацію, службове листування, аналітичні матеріали та інші відомості, поширення яких може впливати на функціонування органів влади або діяльність установ. Кримінально-правова охорона службової інформації спрямована на підтримання належного рівня інформаційної дисципліни та забезпечення стабільності управлінських процесів.

Охорона таємниці засобами кримінального права в Україні охоплює комплекс правових норм, організаційних заходів і діяльність уповноважених органів, спрямованих на захист інформації з обмеженим доступом. Розвиток інформаційного суспільства, цифровізація державних і приватних процесів, поширення електронних комунікацій та зростання кількості інформаційних загроз впливають на подальше вдосконалення кримінально-правових механізмів у сфері охорони таємниці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Берднік І. В., Головка М. Б. Основні орієнтири відмежування колабораційної діяльності від суміжних складів кримінальних правопорушень. *Нове українське право*. 2022. № 2. С. 156-162. DOI: <https://doi.org/10.51989/NUL.2022.2.22>
2. Стратонов В. М. Характеристика державної зради в системі національної безпеки України. *Вісник Національної академії правових наук України*. 2024. Т. 31, № 1. С. 216-233. DOI: <https://doi.org/10.31359/1993-0909-2023-31-1-216>
3. Сервецький І. Суспільна небезпека державної зради під час воєнних дій. *Наукові праці Міжрегіональної Академії управління персоналом*. Юридичні науки. 2022. № 2(62). С. 48-58. DOI: <https://doi.org/10.32689/2522-4603.2022.2.8>
4. Teremetskyi V. I., Bandurka S. S., Korniienko M. V., Dniprov O. S., Slobodeniuk I. V., Albul S. V., Riabchenko Y. Y. Peculiarities of judicial control during pre-trial investigation. *Journal of Ecohumanism*. 2024. Vol. 3, № 8. P. 7375-7384. DOI: <https://doi.org/10.62754/joe.v3i8.5368>
5. Sokurenko V., Levchenko K., Ablamskyi S., de Lima Jr O. P., Šimić G., Romaniuk V. The legal regime of the martial state in Ukraine and its impact on the conduct of pre-trial investigation: new challenges and their overcoming. *Via Inveniendi Et Iudicandi*. 2024. Vol. 19, № 2. P. 92-111. DOI: <https://doi.org/10.15332/10671>
6. Благодарний А. М. Запобігання адміністративним порушенням законодавства про державну таємницю. *Національна безпека: право та економіка*. 2024. № 1. С. 6–13. DOI: <http://doi.org/10.51369/3083-5917-2024-1-1>
7. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>

8. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-ХІІ. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
9. Кодекс України про адміністративні правопорушення: Кодекс Української РСР від 07.12.1984 р. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>
10. Кримінальний кодекс України: Кодекс України від 05.04.2001 р. № 2341-ІІІ. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
11. Про інформацію: Закон України від 02.10.1992 р. № 2657-ХІІ. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
12. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
13. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
14. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-ХІІ. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text>
15. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text>
16. Про державну службу: Закон України від 10.12.2015 р. № 889-VIII. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/889-19#Text>
17. Постанова Кабінету Міністрів України № 1641 від 29.11.2001 р. «Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в

установах і організаціях»: Постанова КМУ від 29.11.2001 р. № 1641. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/1641-2001-п#Text>

18. Постанова Кабінету Міністрів України № 611 від 23.08.1994 р. «Про затвердження Положення про порядок надання допуску до державної таємниці»: Постанова КМУ від 23.08.1994 р. № 611. Редакція станом на 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/611-94-п#Text>

19. Денисовський М. Д., Томчук І. О., Сівіцька Г. Є. Охорона державної таємниці під час кримінального провадження. *Нове українське право*. 2021. Вип. 5. С. 99–104. DOI: <https://doi.org/10.51989/NUL.2021.5.14>

20. Семенюк О. Г. Допуск до державної таємниці як різновид діяльності держави з надання адміністративних послуг. *Інформація і право*. 2017. № 3 (22). С. 94-100. DOI: [https://doi.org/10.37750/2616-6798.2017.3\(22\).273058](https://doi.org/10.37750/2616-6798.2017.3(22).273058)

21. Семенюк О.Г. Державна таємниця як предмет злочину. *Інформація і право*. 2016. № 4 (19). С. 85–94 URL: https://ippi.org.ua/sites/default/files/11_2.pdf

22. Ковальов К.Є., Леонов Б.Д. Забезпечення охорони державної та службової таємниці у сфері оперативно-розшукової діяльності за законодавством окремих держав: порівняльний аналіз. *Інформація і право*. № 1(20)/2017. С. 82-92 URL: <https://ippi.org.ua/kovalov-k%D1%94-leonov-bd-zabezpechennya-okhoroni-derzhavnoi-ta-sluzhbovoi-ta%D1%94mnitsi-u-sferi-operativno-r>

23. Пастернак М. С. Розмежування складів злочину, передбачених ст. 328 «Розголошення державної таємниці» і ст. 329 «Втрата документів, що містять державну таємницю» КК України. *Інформаційна безпека людини, суспільства, держави*. 2018. № 2. С. 20–27 URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=iblsd_2018_2_5

24. Денищук Д.Є. Особливості діяльності державних експертів з питань таємниць Державної кримінально-виконавчої служби України. *Право і безпека*. 2020. № 1 (76). С. 112-117. DOI: <https://doi.org/10.32631/pb.2020.1.16>
25. Денищук Д.Є. Контроль знань з охорони державної таємниці в Державній кримінально-виконавчій службі України: питання сьогодення. *Вісник кримінологічної асоціації України*. 2023. № 1 (28). С. 337-346. DOI: <https://doi.org/10.32631/vca.2023.1.31>
26. Хашев В. Г. Детермінанти розголошення державної таємниці. *Право і суспільство*. 2025. С. 654-659. URL: https://www.pravoisuspilstvo.org.ua/archive/2025/1_2025/97.pdf
27. Сергійчук В. В. Деякі детермінанти розголошення державної таємниці. *Sciences of Europe*. 2020. Vol. 4. No 47. С. 59–63 URL: http://virtuni.education.zp.ua/info_cpu/sites/default/files/diss_Sergiichuk.pdf
28. Миргородська К., Е.В. Копилов. Теоретико-правові основи оперативно-розшукової діяльності в умовах воєнного стану. *Universum*. 2025. С. 74-83. URL: <https://archive.liga.science/index.php/universum/article/view/1636>
29. Антонов, К. В. Проблеми правової охорони інституту державної таємниці у кримінальному провадженні. *Юрид. наук. електрон. журн*. 2020. № 2. С. 355-358. URL: http://www.lsej.org.ua/2_2020/94.pdf.
30. Пузирний В. ДЕРЖАВНА ТАЄМНИЦЯ: ПОНЯТТЯ ТА СУТНІСТЬ. *Актуальні проблеми юридичної науки та практики*, 2021. (1(6), 37–41. URL: <http://aplsp.stu.cn.ua/article/view/229115>
31. Косяченко, Є., Великий, М., Копилов, Е. ПОНЯТТЯ, СУТНІСТЬ, ЗНАЧЕННЯ ТА ОЗНАКИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ. *UNIVERSUM*, 2025. (26), 386–391. URL: <https://archive.liga.science/index.php/universum/article/view/2466>
32. Тищенко Є. Ф. Проблемні аспекти експертизи з питань державної таємниці в кримінальному провадженні. *Криміналістика і судова експертиза*. 2019. Вип. 64. С. 88-101. DOI: <https://doi.org/10.33994/kndise.2019.64.06>

33. Пащенко О. О. Кримінально-правова охорона інформаційної безпеки нормами розділу I Особливої частини КК України. *Питання боротьби зі злочинністю*. 2024. Т. 1, № 47. С. 11-17. DOI: <https://doi.org/10.31359/2079-6242-2024-47-11>

34. Чуваков О. До питання про новели кримінально-правової охорони основ національної безпеки України. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 2(121). С. 298-304. DOI: <https://doi.org/10.31733/2078-3566-2022-6-298-304>

35. Довженко В. Окремі питання кримінально-правової характеристики розголошення державної таємниці. Новітні кримінально-правові дослідження – 2021 : Альманах наукових праць. Миколаїв : МІП НУ ОЮА, 2021. С. 173-177. URL:

<https://ivpz.kh.ua/wpcontent/uploads/2021/05/%D0%90%D0%BB%D1%8C%D0%B%D0%B0%D0%BD%D0%B0%D1%85-2021-%D1%82%D0%B5%D0%BA%D1%81%D1%82.pdf#page=173>