ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД «МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»
ХЕРСОНСЬКИЙ ІНСТИТУТ

КУРСОВА РОБОТА
з дисципліни «Інформаційне право»
на тему: «Охорона державної таємниці в Україні»

Здобувача 4 курсу групи ІН19-9-22-БПр (4,0д)
Напрям підготовки: 08 Право
Спеціальність: 081 Право
Кашула Едуарда Віталійовича
Керівник: канд. політ. наук, доцент
Катеринчук П.М.

Національна шкала: _____
Кількість балів: _____
Оцінка: ECTS _____

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

Чернівці - 2026 р.

ЗМІСТ

ВСТУП

Актуальність теми дослідження охорони державної таємниці в Україні пов’язана зі зростанням ролі інформаційної безпеки у функціонуванні держави, розвитком цифрових технологій та ускладненням сучасного інформаційного середовища. Поширення електронного документообігу, використання цифрових каналів зв’язку та інтеграція інформаційних систем у діяльність органів державної влади супроводжуються підвищенням ризиків несанкціонованого доступу до інформації з обмеженим доступом. Сучасні інформаційні загрози, кіберризики та активне використання цифрових технологій формують потребу у вдосконаленні механізмів захисту секретної інформації та адаптації режиму секретності до нових умов функціонування інформаційного простору.

Ступінь розробки дослідження охоплює праці українських і зарубіжних науковців у сфері інформаційного права, національної безпеки, адміністративного права та організації режиму секретності. Наукові дослідження присвячені визначенню поняття державної таємниці, аналізу системи органів, що забезпечують режим секретності, порядку засекречування інформації, доступу до відомостей з обмеженим доступом та організації контролю за обігом секретної інформації.

Науковці, які досліджували проблематику: 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., Тищенко Є. Ф., Пащенко О. О., Чуваков О., Довженко В., Берднік І.

Мета дослідження полягає у комплексному аналізі теоретико-правових та організаційних засад охорони державної таємниці в Україні.

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

- дослідити поняття та сутність державної таємниці;
- проаналізувати нормативно-правове регулювання охорони державної таємниці;

- охарактеризувати принципи забезпечення режиму секретності в Україні;
- визначити систему органів, що забезпечують охорону державної таємниці;
- дослідити порядок віднесення інформації до державної таємниці та її засекречування;
- проаналізувати порядок доступу до державної таємниці та режим роботи з секретною інформацією;
- визначити основні проблеми функціонування системи захисту державної таємниці;
- дослідити міжнародний досвід забезпечення режиму секретності та можливості його впровадження в Україні;
- охарактеризувати перспективи вдосконалення правового та організаційного механізму охорони державної таємниці.

Об'єктом дослідження є суспільні відносини, що виникають у процесі забезпечення охорони державної таємниці та організації режиму секретності в Україні.

Предметом дослідження є теоретико-правові та організаційні засади охорони державної таємниці в Україні, механізми забезпечення режиму секретності, порядок засекречування інформації, система доступу до секретних відомостей, діяльність органів, що здійснюють захист державної таємниці.

Методи дослідження охоплюють загальнонаукові та спеціально-юридичні методи наукового пізнання. Діалектичний метод використано для аналізу розвитку системи охорони державної таємниці та її функціонування в умовах сучасного інформаційного середовища. Формально-юридичний метод застосовано під час дослідження правових засад режиму секретності та аналізу понять, пов'язаних із захистом інформації з обмеженим доступом.

Структура роботи. Робота складається зі вступу, трьох розділів, які містять дев'ять підрозділів, висновків, списку використаних джерел. Загальний обсяг роботи – 43 сторінки, список використаних джерел – 36 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

1.1. Поняття та сутність державної таємниці

Поняття державної таємниці в Україні формується як правова категорія, що охоплює інформацію, доступ до якої обмежується державою з метою захисту національних інтересів у сферах оборони, безпеки, зовнішньої політики, економіки та інших напрямів функціонування державного механізму. Формування правового режиму базується на визначенні критеріїв віднесення відомостей до категорії секретних, встановленні ступенів секретності та закріпленні процедур контролю за їх обігом.

Державна таємниця охоплює відомості, розголошення яких може вплинути на функціонування державних інституцій або створити загрози для національної безпеки. Законодавство встановлює перелік сфер, у межах яких інформація може бути віднесена до секретної, включаючи військову діяльність, розробку та виробництво озброєння, розвідувальну діяльність, державні запаси, мобілізаційні плани, а також інші напрями, що визначаються уповноваженими органами [1, с.86-87]. Визначення конкретних відомостей здійснюється через процедури класифікації, які передбачають оцінку змісту інформації та можливих наслідків її поширення.

Правовий режим секретності передбачає встановлення трьох ступенів доступу до державної таємниці: «особливої важливості», «цілком таємно» та «таємно». Кожен рівень визначає ступінь обмеження доступу, порядок роботи з інформацією та вимоги до її захисту. Розмежування рівнів здійснюється на основі критеріїв, що враховують характер відомостей і потенційний вплив їх розголошення. Віднесення інформації до певного ступеня секретності оформлюється спеціальними рішеннями уповноважених суб’єктів.

Система охорони державної таємниці включає сукупність органів державної влади, підприємств, установ і організацій, що беруть участь у забезпеченні режиму секретності. До цієї системи належать органи виконавчої влади, Служба безпеки України, підрозділи режимно-секретної діяльності, а також керівні органи суб'єктів, які працюють із секретною інформацією. Розподіл повноважень між цими структурами визначається законодавством і регламентується внутрішніми нормативними актами.

Організація режиму секретності передбачає створення спеціальних умов для обігу інформації, що включає реєстрацію документів, контроль їх переміщення, зберігання у спеціально обладнаних приміщеннях, використання технічних засобів захисту та обмеження доступу до носіїв інформації. Установлення режиму передбачає запровадження внутрішніх інструкцій, що регулюють порядок роботи з документами, а також контроль за їх виконанням.

Доступ до державної таємниці надається фізичним особам після проходження встановлених процедур перевірки. Процес включає оцінку біографічних даних, перевірку відсутності обставин, що перешкоджають доступу, та оформлення допуску відповідного рівня [2, с.84-85]. Надання доступу супроводжується прийняттям зобов'язань щодо нерозголошення інформації, а також ознайомленням із правилами поводження з секретними матеріалами.

Кадрове забезпечення системи охорони державної таємниці включає добір осіб, які отримують доступ до секретної інформації, їх перевірку та підготовку. Процедури перевірки охоплюють аналіз біографічних даних, встановлення зв'язків, що можуть впливати на доступ до інформації, та оцінку надійності. Після отримання допуску працівники підлягають регулярному контролю щодо дотримання вимог режиму секретності.

Інформаційні процеси, пов'язані з державною таємницею, регулюються у взаємодії з іншими правовими інститутами, включаючи захист інформації з обмеженим доступом, регулювання персональних даних та забезпечення кібербезпеки. Взаємодія цих напрямів формує комплексну систему інформаційної безпеки держави, що охоплює різні рівні захисту даних.

Міжнародна практика регулювання секретної інформації демонструє наявність подібних підходів до класифікації, організації доступу та контролю за обігом інформації. Порівняння національних моделей із зарубіжними системами свідчить про використання спільних принципів побудови режиму секретності, адаптованих до особливостей правових систем різних держав.

Адміністративно-правове забезпечення охорони державної таємниці включає регламентацію діяльності органів державної влади, визначення їх повноважень та встановлення відповідальності за порушення режиму секретності. Законодавство передбачає механізми юридичної відповідальності за неправомірне поводження з інформацією, що становить державну таємницю.

Система захисту інформації у сфері державної таємниці функціонує як багаторівнева структура, що охоплює правові, організаційні та технічні заходи. Узгодження дій різних суб'єктів забезпечує функціонування режиму секретності на всіх етапах обігу інформації [3, с.22-23]. Реалізація встановлених процедур формує порядок доступу, використання та зберігання секретних відомостей.

Отже, становлення та розвиток інституту державної таємниці пов'язане з трансформацією інформаційного середовища та змінами у сфері державного управління. Розвиток технологій обробки даних впливає на підходи до захисту інформації та формування нових механізмів забезпечення її конфіденційності. Регулювання у цій сфері передбачає постійне оновлення нормативної бази з урахуванням змін у суспільних та технологічних процесах.

1.2. Нормативно-правове регулювання охорони державної таємниці

Нормативно-правове регулювання охорони державної таємниці в Україні становить систему правових норм, спрямованих на визначення порядку віднесення інформації до категорії секретної, встановлення режиму її використання, зберігання, захисту та розсекречування. Формування цієї системи

відбувається на основі Конституції України [4], міжнародних зобов'язань держави, профільного законодавства та підзаконних нормативних актів, що деталізують процедури у сфері інформації з обмеженим доступом. Правове регулювання охоплює діяльність органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, які працюють з відомостями, що становлять державну таємницю.

Конституція України [4] закріплює базові положення щодо захисту національної безпеки та визначає обов'язок держави забезпечувати збереження інформації, розголошення якої може завдати шкоди інтересам держави. Стаття 17 Конституції України встановлює, що захист суверенітету і територіальної цілісності є справою всього українського народу, а забезпечення інформаційної безпеки входить до функцій держави. Конституційні положення формують основу для подальшого нормативного регулювання режиму секретності.

Базовим спеціальним актом виступає Закон України «Про державну таємницю» [5], який визначає поняття державної таємниці, порядок її охорони, повноваження державних органів у цій сфері, а також встановлює правила класифікації інформації. Закон закріплює критерії віднесення відомостей до державної таємниці, визначає ступені секретності та регламентує процедури засекречування і розсекречування. Окремі положення закону регулюють порядок надання допуску до державної таємниці, встановлюють підстави для його скасування, а також визначають відповідальність за порушення встановленого режиму.

Кодекс України про адміністративні правопорушення [6] містить норми, що передбачають адміністративну відповідальність за порушення порядку поводження з інформацією, яка становить державну таємницю. Статті кодексу регулюють випадки недодержання вимог режиму секретності, порушення правил зберігання документів та інші дії, що створюють загрозу розголошення секретних відомостей. Застосування адміністративних санкцій здійснюється уповноваженими органами відповідно до встановлених процедур.

Кримінальний кодекс України [7] визначає кримінальну відповідальність за дії, пов’язані з розголошенням державної таємниці. Стаття 111 Кримінального кодексу України передбачає відповідальність за державну зраду, що включає передачу іноземній державі, іноземній організації або їх представникам відомостей, які становлять державну таємницю. Стаття 328 Кримінального кодексу України встановлює відповідальність за розголошення державної таємниці особами, яким такі відомості були довірені або стали відомі у зв’язку з виконанням службових обов’язків. Стаття 329 Кримінального кодексу України регулює відповідальність за втрату документів, що містять державну таємницю. Стаття 422 Кримінального кодексу України передбачає відповідальність за розголошення військової інформації, яка становить державну таємницю.

Закон України «Про інформацію» [8] визначає загальні засади правового регулювання інформаційних відносин, включаючи класифікацію інформації за режимом доступу. Положення закону встановлюють, що інформація з обмеженим доступом поділяється на конфіденційну, таємну та службову. Державна таємниця належить до категорії таємної інформації та регулюється спеціальним законодавством. Закон визначає принципи відкритості інформації та підстави для обмеження доступу.

Закон України «Про доступ до публічної інформації» [9] встановлює порядок реалізації права на доступ до інформації, що перебуває у володінні суб’єктів владних повноважень. Положення закону визначають винятки щодо доступу до інформації, яка містить державну таємницю. Обмеження доступу здійснюється на підставі закону, якщо розголошення інформації може завдати шкоди національній безпеці, обороні або іншим інтересам держави.

Закон України «Про національну безпеку України» [10] визначає засади функціонування системи національної безпеки та оборони, включаючи інформаційну безпеку як її складову. Положення закону регулюють діяльність суб’єктів сектору безпеки і оборони, які беруть участь у захисті державної таємниці. Закон визначає роль Служби безпеки України як центрального органу у сфері контррозвідувального захисту інформації з обмеженим доступом.

Закон України «Про Службу безпеки України» [11] регламентує повноваження спеціального органу у сфері охорони державної таємниці. Положення закону визначають функції Служби безпеки України щодо контролю за дотриманням режиму секретності, проведення перевірок, здійснення контррозвідувальних заходів та забезпечення захисту державної інформації. Норми закону закріплюють право органу здійснювати доступ до інформації, що становить державну таємницю, у межах визначених повноважень.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [12] встановлює правові засади захисту інформації, включаючи відомості, що становлять державну таємницю, у електронних системах. Положення закону регулюють вимоги до створення комплексних систем захисту інформації, порядок сертифікації засобів технічного захисту та обов’язки власників інформаційних систем щодо забезпечення безпеки даних.

Закон України «Про державну службу» [13] визначає правовий статус державних службовців, які можуть мати доступ до державної таємниці у зв’язку з виконанням службових обов’язків. Положення закону регулюють питання добору кадрів, проведення спеціальних перевірок, а також встановлюють вимоги до дотримання службової дисципліни та правил поводження з інформацією з обмеженим доступом.

Постанова Кабінету Міністрів України від 29 листопада 2006 року № 1641 «Про затвердження Порядку віднесення інформації до державної таємниці» [14] регулює процедури визначення інформації, що підлягає засекречуванню. Документ встановлює механізм формування та перегляду Зводу відомостей, що становлять державну таємницю, а також порядок підготовки рішень щодо класифікації інформації.

Постанова Кабінету Міністрів України від 18 грудня 2013 року № 939 «Про затвердження Порядку організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях» [15] визначає організаційні засади режиму секретності. Положення документа регулюють порядок створення режимно-секретних

органів, ведення обліку секретних документів, зберігання матеріалів та контроль за їх використанням.

Постанова Кабінету Міністрів України від 23 серпня 1994 року № 611 «Про затвердження Положення про порядок надання допуску до державної таємниці» [16] встановлює процедуру оформлення допуску фізичних осіб до секретної інформації. Документ визначає рівні допуску, підстави для його надання та скасування, а також порядок проведення спеціальної перевірки.

Таким чином, нормативно-правова база охорони державної таємниці формує багаторівневу систему регулювання, що охоплює конституційний, законодавчий, підзаконний та відомчий рівні. Узгодження положень різних нормативних актів забезпечує функціонування єдиного правового режиму секретності, який визначає порядок поводження з інформацією з обмеженим доступом у державі.

1.3. Принципи забезпечення режиму секретності в Україні

Принципи забезпечення режиму секретності в Україні формуються як система базових підходів, що визначають порядок організації захисту інформації з обмеженим доступом, регулювання її обігу та контроль за дотриманням встановлених правил. Функціонування цієї системи пов’язане з необхідністю упорядкування процесів збирання, обробки, зберігання, використання та передачі відомостей, які підлягають спеціальному захисту у зв’язку з їх значенням для державного управління, оборони та безпеки.

Принцип законності визначає здійснення всіх заходів у сфері секретності на основі чітко встановлених правил, які регламентують порядок доступу до інформації, процедури її класифікації та умови використання. Дотримання правових вимог формує єдину систему організації режиму секретності, що виключає довільне застосування обмежень або розширення доступу до

відомостей, які підлягають захисту. Узгодженість дій учасників інформаційних відносин забезпечує стабільність функціонування режиму. Відхилення від встановлених процедур призводить до порушення цілісності системи захисту інформації та ускладнює контроль за її обігом.

Принцип обґрунтованості класифікації інформації передбачає встановлення критеріїв, за якими визначається необхідність обмеження доступу до певних відомостей. Оцінка змісту інформації здійснюється з урахуванням можливих наслідків її поширення для функціонування державних інституцій, оборонної сфери та інших напрямів діяльності, пов'язаних із забезпеченням безпеки. Формування переліків секретної інформації відбувається на основі визначених підходів до аналізу її значущості.

Принцип диференціації рівнів секретності полягає у розподілі інформації за ступенем обмеження доступу. Встановлення різних рівнів пов'язане з необхідністю визначення обсягу обмежень, порядку роботи з матеріалами та вимог до їх захисту. Такий підхід забезпечує упорядкування обігу інформації та визначення відповідних режимів доступу залежно від характеру відомостей [17, с.113-114]. Різні категорії інформації потребують неоднакових заходів захисту, що відображається у структурі режиму секретності.

Принцип обмеження доступу полягає у визначенні кола осіб, які можуть працювати з інформацією, що підлягає захисту. Надання доступу здійснюється після перевірки відповідності встановленим вимогам, що включають оцінку надійності та здатності дотримуватися режимних правил. Обмеження доступу спрямоване на мінімізацію ризиків розголошення відомостей та забезпечення контролю за їх використанням. Система допусків формує багаторівневу структуру доступу до секретних матеріалів.

Принцип персональної відповідальності пов'язаний із встановленням обов'язку осіб, які мають доступ до секретної інформації, дотримуватися визначених правил її обробки та зберігання. Порушення встановленого порядку тягне за собою юридичні наслідки, що визначаються ступенем завданої шкоди та характером дій. Такий підхід формує систему відповідальності за збереження

інформації з обмеженим доступом. Усвідомлення наслідків порушень впливає на поведінку учасників інформаційних процесів. Регламентація відповідальності підтримує дисципліну у сфері обігу секретних відомостей.

Принцип організаційної структурованості передбачає функціонування системи органів і підрозділів, які здійснюють управління режимом секретності. Розподіл функцій між різними рівнями управління забезпечує координацію дій у сфері захисту інформації та контроль за дотриманням встановлених правил. Взаємодія між суб'єктами системи спрямована на підтримання єдиного порядку обігу секретних відомостей. Чітке визначення повноважень сприяє уникненню дублювання функцій. Узгодженість управлінських процесів впливає на ефективність функціонування системи захисту інформації.

Принцип обмеженості строку дії режиму секретності полягає у тимчасовому характері обмеження доступу до інформації. Перегляд доцільності подальшого збереження режиму здійснюється на основі аналізу актуальності відомостей та їх значення для державних інтересів. Після втрати необхідності обмеження інформація переходить у відкритий обіг. Процедури перегляду сприяють оновленню інформаційних ресурсів держави [18, с.338-339]. Зміна статусу інформації впливає на структуру інформаційного середовища.

Принцип захисту інформаційного середовища передбачає використання сукупності заходів, спрямованих на забезпечення безпеки даних у процесі їх обробки та передачі. Захист охоплює як традиційні носії інформації, так і електронні системи, що використовуються для зберігання та передачі відомостей. Застосування технічних засобів спрямоване на запобігання несанкціонованому доступу. Розвиток цифрових технологій ускладнює процеси захисту інформації та потребує вдосконалення методів контролю. Інтеграція технічних рішень у систему захисту підвищує рівень інформаційної безпеки.

Отже, сукупність принципів забезпечення режиму секретності формує основу організації захисту інформації з обмеженим доступом, визначає порядок функціонування відповідних механізмів та структурує діяльність суб'єктів, які беруть участь у збереженні інформаційної безпеки держави. Застосування цих

принципів впливає на стабільність інформаційного середовища та забезпечує впорядкування процесів обігу секретних відомостей. Взаємодія різних підходів створює цілісну систему регулювання у сфері інформаційної безпеки.

Висновки до розділу 1

Теоретико-правові основи охорони державної таємниці в Україні формують систему базових наукових підходів і правових конструкцій, що визначають сутність, структуру та функціонування режиму секретності. У межах цієї системи розкриваються поняття державної таємниці, критерії віднесення інформації до категорії секретної, принципи її захисту, а також загальні засади організації доступу та контролю. Теоретичне осмислення цих положень забезпечує узгодженість між різними елементами правового регулювання, включаючи конституційні норми, спеціальне законодавство та підзаконні акти.

Практичне значення теоретико-правових основ проявляється у забезпеченні стабільного функціонування механізмів захисту інформації з обмеженим доступом, організації діяльності уповноважених органів та встановленні єдиних стандартів поводження з секретними відомостями. Розробка та застосування теоретичних положень впливає на формування ефективних процедур класифікації інформації, визначення рівнів секретності та встановлення правил доступу до неї. Системність теоретичних засад сприяє узгодженню правозастосовної практики, підвищенню рівня організації режиму секретності та забезпеченню взаємодії між різними суб’єктами, що беруть участь у процесах охорони державної таємниці.

РОЗДІЛ 2
ОРГАНІЗАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

2.1. Система органів, що забезпечують охорону державної таємниці

Система органів, що забезпечують охорону державної таємниці в Україні, являє собою сукупність державних інституцій, підрозділів та посадових осіб, на яких покладено функції організації, контролю та реалізації заходів щодо захисту інформації з обмеженим доступом. Формування цієї системи відбувається у межах загальної архітектури державного управління та інформаційної безпеки, де визначаються напрями роботи із секретними відомостями, порядок їх обігу та механізми контролю. Структура системи охоплює різні рівні управління, що забезпечують функціонування режиму секретності у державі.

Центральне місце у системі органів охорони державної таємниці займає спеціально уповноважений державний орган у сфері безпеки, діяльність якого пов’язана з контррозвідувальним захистом інформації. У межах його повноважень здійснюється контроль за дотриманням режиму секретності, організація перевірок, участь у формуванні вимог до захисту інформації та реалізація заходів із запобігання витоку секретних відомостей [19, с.655-656]. Взаємодія з іншими органами державної влади відбувається у форматі координації та обміну інформацією, що стосується захисту державних інтересів.

Координаційні функції у сфері охорони державної таємниці здійснюються через систему виконавчої влади, яка забезпечує формування та реалізацію державної політики у сфері інформаційної безпеки. На цьому рівні визначаються загальні підходи до організації режиму секретності, порядок роботи з інформацією з обмеженим доступом, а також механізми взаємодії між різними суб’єктами системи. Управлінські рішення спрямовані на забезпечення узгодженості дій у межах державного механізму.

Галузеві органи виконавчої влади формують внутрішні системи забезпечення охорони державної таємниці відповідно до специфіки своєї діяльності. У структурі таких органів функціонують підрозділи, що відповідають за організацію роботи з секретною інформацією, контроль за її обігом та дотримання встановлених процедур. Регламентація внутрішніх процесів охоплює ведення обліку документів, організацію доступу до інформації та забезпечення її зберігання у визначеному порядку.

На підприємствах, в установах та організаціях, які працюють із секретною інформацією, створюються спеціальні підрозділи або визначаються відповідальні особи. Їх діяльність пов’язана з організацією режимних заходів, контролем за використанням інформації та забезпеченням дотримання встановлених правил. Керівники таких суб’єктів відповідають за створення умов, необхідних для функціонування режиму секретності, та організацію внутрішнього контролю.

Органи місцевого самоврядування у випадках роботи з інформацією обмеженого доступу виконують функції забезпечення режиму секретності у межах наданих повноважень. Організація роботи з такими відомостями здійснюється відповідно до загальних вимог системи захисту інформації. Взаємодія з органами державної влади забезпечує узгодженість дій у сфері інформаційної безпеки на місцевому рівні [20, с.60-61].

Судові та правоохоронні органи беруть участь у функціонуванні системи охорони державної таємниці через здійснення правозастосовної діяльності та контроль за дотриманням встановлених правил. Розгляд справ, пов’язаних із порушенням режиму секретності, здійснюється з урахуванням необхідності захисту інформації обмеженого доступу. У межах кримінального провадження забезпечується дотримання спеціальних процедур роботи з матеріалами, що містять секретні відомості.

Система внутрішнього контролю в органах, що працюють із державною таємницею, передбачає перевірку стану організації режиму секретності, дотримання правил обліку документів та умов їх зберігання. Контрольні заходи

здійснюються керівниками структурних підрозділів та спеціально призначеними посадовими особами. Зовнішній контроль реалізується уповноваженими державними органами шляхом проведення перевірок та оцінки стану режимної роботи.

Технічний компонент системи охорони державної таємниці пов’язаний із використанням засобів захисту інформації, що обробляється в електронних системах. Використання криптографічних методів, систем контролю доступу та програмно-апаратних комплексів спрямоване на запобігання несанкціонованому доступу до інформаційних ресурсів. Захист охоплює як передачу даних, так і їх зберігання у цифрових середовищах.

Взаємодія між органами, що забезпечують охорону державної таємниці, здійснюється через координаційні механізми, які передбачають обмін інформацією, узгодження дій та проведення спільних заходів. Така взаємодія формує цілісність системи та забезпечує узгодженість функціонування її складових [21, с.75-76]. Розподіл функцій між суб’єктами сприяє впорядкуванню процесів захисту інформації.

Таким чином, система органів охорони державної таємниці функціонує як багаторівневий механізм, у якому поєднуються управлінські, контрольні, організаційні та технічні елементи. Узгодженість дій між різними рівнями забезпечує стабільність режиму секретності та охоплює всі етапи обігу інформації з обмеженим доступом.

2.2. Порядок віднесення інформації до державної таємниці та її засекречування

Порядок віднесення інформації до державної таємниці та її засекречування в Україні становить регламентовану систему процедур, спрямовану на визначення відомостей, що потребують обмеження доступу, встановлення рівня

їх секретності та організацію режиму захисту. Формування цього порядку базується на загальних засадах державного управління у сфері інформаційної безпеки та охоплює діяльність органів, установ і посадових осіб, які працюють з інформацією підвищеної чутливості. У процесі реалізації таких процедур враховується значення інформації для функціонування державних інституцій, оборонної сфери, зовнішніх відносин та інших напрямів діяльності, пов'язаних із забезпеченням стабільності державних процесів.

Віднесення інформації до категорії, що підлягає обмеженому доступу, здійснюється на основі аналізу її змісту та потенційних наслідків поширення. Оцінка охоплює характер відомостей, їх джерела походження, ступінь деталізації та можливий вплив на діяльність державних органів. Формування рішення щодо класифікації передбачає узагальнення даних, які надходять від різних суб'єктів, що володіють відповідною інформацією, та визначення доцільності встановлення режиму секретності [22, с.356-357]. У цьому процесі враховується взаємозв'язок інформації з іншими масивами даних, що можуть мати значення для державного управління.

Система класифікації інформації передбачає поділ на кілька рівнів секретності залежно від ступеня можливого впливу її розголошення. Встановлення рівня секретності визначає характер обмежень, що застосовуються до інформації, та порядок роботи з нею. Різні категорії інформації потребують різного рівня захисту, що відображається у структурі режиму обігу секретних відомостей. Визначення рівня секретності супроводжується документальним оформленням та фіксацією відповідного статусу інформації.

Процедура засекречування передбачає запровадження режиму обмеженого доступу до визначених відомостей. У процесі засекречування встановлюється коло осіб, які мають право працювати з інформацією, а також визначаються умови її зберігання, обробки та передачі. Формування режиму супроводжується створенням організаційних механізмів контролю, що забезпечують дотримання встановлених вимог. Облік інформації здійснюється для фіксації її руху та контролю за використанням.

Зберігання інформації, що підлягає обмеженому доступу, організовується у спеціально визначених умовах, які виключають несанкціоноване втручання. Для цього застосовуються фізичні та організаційні заходи, спрямовані на обмеження доступу до носіїв інформації. Контроль за переміщенням документів забезпечує збереження їх цілісності та запобігає втраті або несанкціонованому копіюванню. Важливим елементом є реєстрація всіх операцій, пов'язаних із рухом секретних матеріалів.

Допуск до інформації з обмеженим доступом надається після перевірки відповідності осіб встановленим вимогам. Процедура включає оцінку їх надійності, аналіз біографічних даних та визначення рівня доступу, необхідного для виконання службових обов'язків. Надання допуску супроводжується встановленням персональної відповідальності за дотримання режиму секретності та нерозголошення інформації.

Контроль за дотриманням порядку засекречування здійснюється шляхом перевірки правильності класифікації інформації, виконання процедур обліку та дотримання правил її зберігання. Перевірки охоплюють діяльність органів державної влади, підприємств та установ, що працюють із секретними відомостями. Результати контрольних заходів використовуються для коригування організаційних процесів та вдосконалення механізмів захисту інформації.

Розсекречування інформації відбувається у випадках, коли зникає необхідність у подальшому обмеженні доступу. Процедура передбачає перегляд рішень щодо класифікації та оцінку актуальності відомостей. Після зняття обмежень інформація переходить у відкритий обіг відповідно до встановленого порядку [23, с.38-39]. Зміна статусу інформації фіксується у відповідних документах та системах обліку.

Відповідальність за порушення порядку засекречування охоплює випадки неправомірного розголошення інформації, порушення правил її зберігання або втрати документів. Застосування санкцій залежить від характеру порушення та його наслідків. Контроль за дотриманням вимог режиму секретності

спрямований на запобігання таким випадкам та забезпечення стабільності системи захисту інформації.

Технічні засоби захисту інформації використовуються для забезпечення безпеки даних у процесі їх обробки та передачі. Застосування систем шифрування, контролю доступу та моніторингу інформаційних потоків спрямоване на зниження ризиків несанкціонованого доступу. Захист охоплює як електронні, так і паперові носії інформації, що містять відомості з обмеженим доступом.

Порядок віднесення інформації до державної таємниці функціонує у взаємодії з іншими режимами доступу до інформації, що визначають рівень відкритості або конфіденційності даних. Розмежування інформаційних режимів забезпечує впорядкування інформаційних процесів та визначення чітких меж доступу до відомостей.

Система засекречування має багаторівневий характер, що охоплює організаційні, технічні та кадрові елементи. Узгодженість дій різних суб'єктів забезпечує стабільність режиму секретності та контроль за обігом інформації на всіх етапах її життєвого циклу. Організаційний рівень включає формування внутрішніх структур, які відповідають за облік, зберігання та передачу відомостей з обмеженим доступом, а також встановлення процедур взаємодії між підрозділами, що працюють із секретними матеріалами [24, с.387-388].

Отже, функціонування кожного рівня передбачає взаємозалежність між ними, оскільки порушення в одному елементі впливає на ефективність усієї системи. Організаційні процедури визначають порядок роботи з інформацією, технічні засоби забезпечують її фізичний та цифровий захист, а кадрові механізми формують коло осіб, які мають право доступу до відповідних даних. Сукупність цих складових створює єдиний механізм контролю, що охоплює всі етапи обігу інформації від її створення до архівного зберігання або розсекречування. Взаємодія між рівнями забезпечує узгодженість дій та підтримання встановленого режиму обмеженого доступу.

2.3. Доступ до державної таємниці та режим роботи з секретною інформацією

Доступ до державної таємниці та режим роботи з секретною інформацією в Україні становлять систему процедур і організаційних заходів, спрямованих на регулювання порядку використання відомостей з обмеженим доступом, визначення кола осіб, які мають право працювати з такими матеріалами, та забезпечення контролю за їх обігом. Формування цієї системи пов'язане з необхідністю захисту інформації, розголошення якої може вплинути на функціонування державних інституцій, оборонної сфери, зовнішньополітичної діяльності та інших напрямів забезпечення національної безпеки.

Доступ до державної таємниці надається виключно особам, діяльність яких пов'язана з необхідністю використання секретної інформації під час виконання службових обов'язків. Надання доступу передбачає проведення перевірки, у межах якої здійснюється оцінка відповідності особи встановленим вимогам, аналіз біографічних даних, професійної підготовки та інших факторів, що можуть впливати на дотримання режиму секретності. Результати перевірки використовуються для прийняття рішення щодо можливості роботи з інформацією певного рівня секретності [25, с.92-94].

Система доступу до державної таємниці побудована на принципі диференціації рівнів секретності інформації. Рівень доступу визначається залежно від характеру відомостей, обсягу службових повноважень особи та необхідності використання конкретних матеріалів у процесі виконання професійних функцій. Розмежування рівнів доступу спрямоване на мінімізацію ризиків розголошення інформації та впорядкування процесу її використання. Формування багаторівневої структури доступу забезпечує контроль за обігом секретних відомостей у різних сферах державного управління.

Особи, які отримують доступ до державної таємниці, зобов'язані дотримуватися встановлених правил роботи з інформацією обмеженого доступу.

Виконання таких правил охоплює порядок ознайомлення з документами, умови їх використання, передачі та зберігання. Порушення режимних вимог створює ризики втрати контролю над інформацією та може призвести до її несанкціонованого поширення. У зв’язку з цим організація роботи з секретними матеріалами передбачає суворе регламентування дій осіб, які мають відповідний допуск.

Режим роботи з секретною інформацією включає ведення спеціального обліку документів та інших носіїв інформації. Реєстрація матеріалів здійснюється для забезпечення контролю за їх переміщенням, використанням та зберіганням. Кожен документ підлягає фіксації у відповідних системах обліку, що дає можливість визначити місцезнаходження матеріалів та коло осіб, які працювали з ними. Контроль за рухом документів спрямований на забезпечення їх цілісності та запобігання втраті.

Зберігання секретної інформації організовується у спеціально визначених приміщеннях, обладнаних засобами фізичного та технічного захисту. Використання систем контролю доступу, сигналізації та інших засобів безпеки спрямоване на обмеження можливості несанкціонованого проникнення до місць зберігання інформації. Режимні приміщення функціонують відповідно до встановлених вимог, що регламентують порядок перебування осіб, використання технічних засобів та обіг документів [26, с.12-13].

Робота з електронною секретною інформацією передбачає застосування спеціалізованих засобів технічного захисту. Використання криптографічних методів, захищених каналів зв’язку та систем контролю доступу забезпечує безпеку інформаційних потоків у процесі передачі та обробки даних. Організація електронного документообігу у сфері секретної інформації потребує впровадження окремих режимних процедур, пов’язаних із використанням комп’ютерних систем та мереж.

Передача секретної інформації між органами державної влади, установами та іншими суб’єктами здійснюється відповідно до встановлених процедур, що визначають порядок транспортування документів, використання спеціальних

засобів зв’язку та умови збереження конфіденційності. У процесі передачі інформації застосовуються заходи контролю, спрямовані на виключення ризиків втрати матеріалів або несанкціонованого доступу до них. Кожен етап передачі підлягає документальному оформленню та фіксації у системах обліку.

Організація режиму секретності передбачає проведення інструктажів та підготовки осіб, які працюють із секретною інформацією. Навчання охоплює порядок роботи з документами, правила використання технічних засобів захисту, вимоги щодо поведінки у режимних приміщеннях та дії у випадках виникнення загроз інформаційній безпеці. Підготовка персоналу спрямована на формування навичок дотримання встановлених процедур та підтримання належного рівня дисципліни.

Порушення правил доступу до державної таємниці або режиму роботи з секретною інформацією тягне за собою юридичні наслідки залежно від характеру порушення та ступеня завданої шкоди. Розголошення інформації, втрата документів або порушення правил їх використання створюють загрозу для інформаційної безпеки держави та можуть впливати на діяльність державних інституцій. У зв’язку з цим система режимних заходів передбачає персональну відповідальність осіб, які мають доступ до секретних відомостей.

Використання сучасних інформаційних технологій впливає на організацію режиму роботи з секретною інформацією та потребує вдосконалення методів захисту даних. Поширення електронного документообігу, використання цифрових систем зв’язку та інтеграція інформаційних ресурсів ускладнюють процес забезпечення конфіденційності інформації [27, с.299-300]. У зв’язку з цим застосовуються додаткові технічні та організаційні заходи, спрямовані на підтримання безпеки інформаційного середовища.

Таким чином, система доступу до державної таємниці та режим роботи з секретною інформацією функціонує як багаторівневий механізм, що охоплює кадрові, організаційні та технічні складові. Узгодженість дій між різними елементами системи забезпечує контроль за обігом інформації з обмеженим

доступом та підтримання встановленого режиму секретності на всіх етапах роботи з відомостями.

Висновки до розділу 2

Організаційно-правовий механізм охорони державної таємниці формує систему взаємопов’язаних елементів, що забезпечують регулювання процесів захисту інформації з обмеженим доступом, визначення порядку її використання та контроль за дотриманням режиму секретності. У межах цього механізму поєднуються діяльність державних органів, внутрішньовідомчі процедури, кадрове забезпечення, технічні засоби захисту та правила роботи з інформаційними ресурсами. Формування чіткої організаційної структури сприяє впорядкуванню процесів обігу секретної інформації, координації дій між різними суб’єктами та підтриманню стабільності функціонування системи інформаційної безпеки. Правові норми визначають межі повноважень органів державної влади, порядок надання доступу до секретних відомостей і відповідальність за порушення встановленого режиму.

Практичне значення організаційно-правового механізму охорони державної таємниці пов’язане із забезпеченням належного рівня контролю за використанням інформації, що має значення для державного управління, оборонної сфери та безпеки. Реалізація режимних заходів охоплює організацію спеціального діловодства, використання систем контролю доступу, проведення перевірок та підготовку осіб, які працюють із секретними матеріалами. Узгодженість правових і організаційних елементів впливає на ефективність функціонування системи захисту інформації та підтримання визначеного порядку роботи з відомостями обмеженого доступу. Взаємодія між різними складовими механізму забезпечує цілісність режиму секретності та стабільність інформаційного середовища держави.

РОЗДІЛ 3
ПРОБЛЕМИ ТА НАПРЯМИ УДОСКОНАЛЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

3.1. Основні проблеми функціонування системи захисту державної таємниці

Функціонування системи захисту державної таємниці в Україні супроводжується низкою проблем, що пов’язані з організаційними, кадровими, технічними та інформаційними чинниками. Складність сучасного інформаційного середовища впливає на стабільність режиму секретності та ускладнює контроль за обігом відомостей з обмеженим доступом. Зростання обсягів електронного документообігу, поширення цифрових засобів зв’язку та інтеграція інформаційних систем формують нові ризики для захисту секретної інформації. Використання сучасних технологій супроводжується підвищенням імовірності несанкціонованого доступу до інформаційних ресурсів, втручання у роботу електронних систем та незаконного копіювання даних [28, с.174-175]. У зв’язку з цим постає потреба постійного оновлення технічних засобів захисту та вдосконалення механізмів контролю за інформаційними потоками.

Однією з проблем функціонування системи захисту державної таємниці є складність організації ефективного контролю за доступом до інформації. Розширення кола осіб, які працюють із секретними матеріалами, збільшує ризики порушення режиму секретності та ускладнює процеси внутрішнього контролю. У межах окремих установ виникають труднощі, пов’язані з належним обліком документів, фіксацією їх переміщення та перевіркою дотримання встановлених процедур. Недостатній рівень координації між структурними підрозділами може призводити до втрати цілісності системи захисту інформації та виникнення прогалин у режимній роботі.

Кадровий аспект функціонування системи захисту державної таємниці пов’язаний із необхідністю забезпечення належного рівня професійної підготовки осіб, які працюють із секретною інформацією. Низький рівень обізнаності щодо правил режиму секретності, помилки під час роботи з документами та недотримання процедур створюють ризики розголошення відомостей. Організація підготовки персоналу потребує постійного оновлення навчальних програм відповідно до змін у сфері інформаційної безпеки та розвитку цифрових технологій. Плинність кадрів у певних сферах державного управління впливає на стабільність функціонування режиму секретності та ускладнює підтримання належного рівня дисципліни.

Технічні проблеми системи захисту державної таємниці пов’язані зі станом інформаційної інфраструктури та рівнем захищеності електронних систем. Використання застарілого обладнання, недостатній рівень модернізації програмного забезпечення та обмеженість ресурсів для оновлення засобів захисту впливають на безпеку інформаційного середовища. Кіберзагрози, спрямовані на отримання доступу до державних інформаційних ресурсів, потребують застосування складних систем технічного захисту та постійного моніторингу мережевої активності [29, с.158-159]. Ускладнення способів несанкціонованого втручання у роботу електронних систем вимагає вдосконалення механізмів реагування на кіберінциденти.

Організаційні труднощі виникають у процесі взаємодії між різними органами та установами, що працюють із секретною інформацією. Відмінності у внутрішніх процедурах, рівнях технічного забезпечення та підходах до організації режимної роботи можуть впливати на узгодженість дій між суб’єктами системи захисту інформації. Наявність великої кількості інформаційних ресурсів у різних сферах державного управління ускладнює процес централізованого контролю та координації режимних заходів. Розмежування повноважень між різними структурними елементами іноді супроводжується дублюванням функцій або недостатньою визначеністю відповідальності.

Проблеми у сфері захисту державної таємниці пов’язані і з людським фактором, який залишається одним із найбільш поширених джерел порушень режиму секретності. Неналежне виконання службових обов’язків, недотримання вимог щодо зберігання документів, порушення правил користування технічними засобами та передача інформації через незахищені канали зв’язку створюють ризики витоку відомостей. Випадки втрати документів або неналежного поводження з електронними носіями інформації впливають на стабільність системи захисту та потребують посилення внутрішнього контролю.

Складність функціонування системи захисту державної таємниці зростає у зв’язку з розвитком міжнародного інформаційного обміну та інтеграцією цифрових технологій у державне управління. Використання глобальних комунікаційних мереж створює додаткові ризики для захисту секретної інформації та потребує впровадження спеціальних механізмів безпеки. Передача інформації між різними суб’єктами супроводжується необхідністю забезпечення конфіденційності даних та контролю за умовами їх використання.

Проблеми функціонування системи захисту державної таємниці охоплюють і питання підтримання балансу між режимом секретності та потребою забезпечення доступу до інформації у сфері державного управління. Надмірне обмеження доступу може ускладнювати інформаційний обмін між органами влади та впливати на оперативність прийняття управлінських рішень. Водночас недостатній рівень обмежень підвищує ризики несанкціонованого поширення інформації [30, с.222-224]. Формування збалансованого підходу до класифікації відомостей потребує постійного перегляду критеріїв засекречування та оцінки актуальності встановлених обмежень.

Таким чином, функціонування системи захисту державної таємниці в умовах сучасного інформаційного середовища потребує постійного вдосконалення організаційних, кадрових і технічних механізмів. Зміни у сфері цифрових технологій, ускладнення інформаційних потоків та зростання кількості кіберзагроз впливають на структуру режимних заходів і вимагають адаптації системи захисту до нових умов. Узгодженість дій між різними

суб’єктами, оновлення технічної інфраструктури та підвищення рівня підготовки персоналу залишаються складовими стабільного функціонування режиму секретності.

3.2. Міжнародний досвід забезпечення режиму секретності та можливості його впровадження в Україні

Міжнародний досвід забезпечення режиму секретності формується під впливом розвитку інформаційних технологій, трансформації систем державного управління та посилення вимог до захисту інформації у сфері безпеки й оборони. У багатьох державах функціонують комплексні системи захисту секретної інформації, що поєднують організаційні, кадрові та технічні механізми контролю за обігом відомостей з обмеженим доступом. Організація режиму секретності базується на принципах багаторівневого доступу до інформації, персональної відповідальності посадових осіб та постійного моніторингу інформаційного середовища. Використання сучасних цифрових технологій впливає на структуру режимних заходів і формує нові підходи до організації захисту інформаційних ресурсів.

У державах Європейського Союзу система захисту секретної інформації пов’язана з функціонуванням спеціалізованих органів, що здійснюють координацію режимних заходів, контроль за доступом до інформації та перевірку осіб, які працюють із секретними матеріалами. Організація роботи з відомостями обмеженого доступу супроводжується використанням електронних систем обліку документів, захищених каналів зв’язку та криптографічних засобів захисту даних [31, с.49-50]. Режимні процедури охоплюють усі етапи обігу інформації – від її створення до архівного зберігання або розсекречування. Високий рівень автоматизації процесів обробки інформації сприяє підвищенню контролю за використанням секретних матеріалів.

Практика держав Північноатлантичного альянсу характеризується застосуванням уніфікованих стандартів захисту інформації та координацією дій між державними органами різних країн. Система доступу до секретної інформації ґрунтується на багаторівневій структурі допуску, у межах якої кожна особа отримує доступ виключно до відомостей, необхідних для виконання службових обов'язків. Організація режиму секретності супроводжується постійною перевіркою рівня захищеності інформаційних систем та проведенням аудитів інформаційної безпеки. Використання єдиних стандартів забезпечує узгодженість процедур між державами та підтримання спільного режиму захисту інформації.

Досвід Сполучених Штатів Америки пов'язаний із функціонуванням розгалуженої системи захисту секретної інформації, що охоплює військову, розвідувальну та цивільну сфери державного управління. Організація режиму секретності включає застосування складних процедур перевірки осіб, які отримують доступ до секретних матеріалів, використання сучасних систем кіберзахисту та постійний моніторинг інформаційних потоків. Значна увага приділяється технічному захисту електронних ресурсів та контролю за використанням цифрових засобів зв'язку [32]. Підхід до забезпечення інформаційної безпеки базується на інтеграції кадрових, організаційних та технічних елементів у межах єдиної системи контролю.

У країнах Азії спостерігається активне впровадження цифрових технологій у систему забезпечення режиму секретності. Використання систем штучного інтелекту, автоматизованого моніторингу та багаторівневих електронних засобів ідентифікації спрямоване на підвищення контролю за доступом до інформації. Організація роботи з секретними даними супроводжується впровадженням централізованих електронних платформ, що забезпечують облік документів та контроль за їх використанням. Розвиток цифрової інфраструктури впливає на зміну підходів до організації режимних процедур та посилення захисту інформаційних систем.

Можливості впровадження міжнародного досвіду в Україні пов’язані з адаптацією сучасних підходів до організації режиму секретності та вдосконаленням системи захисту інформації. Використання електронних систем обліку секретних документів може сприяти підвищенню контролю за обігом інформації та скороченню ризиків втрати матеріалів. Інтеграція сучасних засобів криптографічного захисту та систем контролю доступу впливає на рівень безпеки електронних інформаційних ресурсів. Розвиток цифрових механізмів захисту інформації потребує оновлення технічної інфраструктури та підготовки персоналу до роботи з новими технологіями.

Запровадження міжнародних підходів до кадрової політики у сфері захисту державної таємниці може сприяти вдосконаленню процедур перевірки осіб, які отримують доступ до секретної інформації. У багатьох державах застосовується система періодичного перегляду допусків, психологічного оцінювання персоналу та контролю за дотриманням режимних вимог у процесі професійної діяльності. Використання подібних механізмів в Україні впливає на стабільність функціонування режиму секретності та підтримання належного рівня дисципліни у сфері роботи з інформацією обмеженого доступу [33].

Міжнародний досвід у сфері кібербезпеки має значення для вдосконалення системи захисту державної таємниці в умовах розвитку цифрових технологій. Використання сучасних систем моніторингу мережевої активності, виявлення кіберзагроз та реагування на інформаційні інциденти сприяє підвищенню рівня захищеності державних інформаційних ресурсів. Формування спеціалізованих центрів кіберзахисту та інтеграція їх діяльності у загальну систему інформаційної безпеки впливає на ефективність реагування на сучасні загрози.

Процес впровадження міжнародного досвіду в Україні пов’язаний із необхідністю врахування національних особливостей організації державного управління, структури інформаційних систем та кадрового забезпечення. Адаптація іноземних моделей потребує узгодження технічних, організаційних та кадрових механізмів із внутрішніми потребами держави. Взаємодія з міжнародними партнерами у сфері інформаційної безпеки сприяє обміну

практичним досвідом та формуванню сучасних підходів до захисту секретної інформації.

Отже, міжнародний досвід забезпечення режиму секретності свідчить про тенденцію до поєднання традиційних режимних процедур із сучасними цифровими технологіями та багаторівневими системами контролю. Використання комплексних підходів до захисту інформації впливає на організацію роботи з секретними матеріалами та підтримання стабільності інформаційного середовища. Впровадження окремих елементів міжнародної практики в Україні може сприяти модернізації системи охорони державної таємниці та адаптації її до умов сучасного інформаційного простору.

3.3. Перспективи вдосконалення правового та організаційного механізму охорони державної таємниці

Перспективи вдосконалення правового та організаційного механізму охорони державної таємниці в Україні пов’язані з розвитком інформаційного середовища, поширенням цифрових технологій та зміною підходів до забезпечення інформаційної безпеки. Сучасні умови функціонування державних інституцій супроводжуються постійним збільшенням обсягів інформації, що обробляється в електронній формі, розширенням каналів комунікації та інтеграцією цифрових систем у сферу державного управління. У зв’язку з цим виникає потреба адаптації механізмів захисту інформації до нових умов функціонування інформаційних ресурсів та вдосконалення процедур контролю за їх використанням [34, с.7-8]. Розвиток системи охорони державної таємниці пов’язаний із необхідністю поєднання правових, організаційних і технічних засобів у межах єдиного механізму забезпечення режиму секретності.

Перспективним напрямом удосконалення організаційного механізму охорони державної таємниці є модернізація системи обліку та контролю за обігом

секретної інформації. Використання електронних платформ для реєстрації документів, фіксації їх переміщення та контролю за доступом до матеріалів сприяє впорядкуванню режимних процедур і підвищенню рівня контролю за використанням інформації. Інтеграція автоматизованих систем у діяльність органів державної влади впливає на швидкість обробки інформації та підтримання належного рівня захищеності інформаційних ресурсів. Формування централізованих механізмів контролю за інформаційними потоками спрямоване на зниження ризиків втрати документів та несанкціонованого доступу до відомостей.

Удосконалення кадрового забезпечення системи охорони державної таємниці пов’язане з підвищенням рівня професійної підготовки осіб, які працюють із секретною інформацією. Організація спеціалізованого навчання у сфері режиму секретності, кібербезпеки та технічного захисту інформації впливає на якість виконання службових обов’язків та дотримання встановлених процедур. Розвиток системи підготовки персоналу охоплює оновлення навчальних програм відповідно до сучасних інформаційних загроз та використання практичних механізмів оцінки рівня знань працівників [35, с.101-102]. Формування стабільного кадрового складу сприяє підтриманню безперервності функціонування системи захисту інформації.

Перспективи розвитку правового механізму охорони державної таємниці пов’язані з удосконаленням процедур класифікації інформації та переглядом підходів до визначення рівнів секретності. Зміни у структурі інформаційного середовища впливають на зміст відомостей, які потребують обмеження доступу, та формують потребу у регулярному оновленні критеріїв засекречування. Формування чітких процедур перегляду статусу інформації спрямоване на підтримання балансу між режимом секретності та інформаційними потребами державного управління. Узгодженість правових механізмів із сучасними умовами функціонування цифрових систем впливає на стабільність правового регулювання у сфері інформаційної безпеки.

Розвиток технічного компоненту системи охорони державної таємниці пов’язаний із впровадженням сучасних засобів кіберзахисту та моніторингу інформаційного середовища. Використання систем виявлення кіберзагроз, багаторівневого контролю доступу та засобів криптографічного захисту спрямоване на підвищення безпеки електронних інформаційних ресурсів. Розширення використання цифрових технологій у державному секторі потребує вдосконалення механізмів захисту каналів передачі даних та створення стійкої інформаційної інфраструктури. Розвиток технічних засобів контролю впливає на здатність системи реагувати на сучасні інформаційні загрози.

Перспективним напрямом розвитку організаційного механізму є вдосконалення взаємодії між органами державної влади, підприємствами та установами, що працюють із секретною інформацією. Координація дій між різними суб’єктами системи захисту інформації сприяє впорядкуванню режимних процедур та підтриманню єдиного підходу до організації роботи з відомостями обмеженого доступу [36, с.95-96]. Формування спільних стандартів обліку, передачі та зберігання інформації впливає на узгодженість діяльності різних структурних елементів системи охорони державної таємниці.

Міжнародна співпраця у сфері інформаційної безпеки формує додаткові перспективи вдосконалення механізмів охорони державної таємниці. Обмін досвідом із зарубіжними державами, використання сучасних технологій захисту інформації та впровадження міжнародних підходів до організації режиму секретності сприяють модернізації національної системи захисту інформації. Участь у міжнародних програмах та професійних платформах впливає на розвиток кадрового потенціалу та адаптацію сучасних методів роботи з секретними матеріалами.

Таким чином, подальший розвиток системи охорони державної таємниці в Україні пов’язаний із поєднанням організаційних, кадрових, правових і технічних напрямів удосконалення. Комплексний підхід до модернізації режиму секретності охоплює оновлення інформаційної інфраструктури, розвиток цифрових механізмів контролю, вдосконалення процедур доступу до інформації

та підвищення рівня професійної підготовки персоналу. Узгодженість дій між різними елементами системи впливає на стабільність функціонування режиму секретності та адаптацію механізмів захисту інформації до сучасних умов інформаційного середовища.

Висновки до розділу 3

Проблеми та напрями удосконалення системи охорони державної таємниці в Україні пов’язані з необхідністю адаптації механізмів захисту інформації до сучасних умов розвитку інформаційного середовища та цифрових технологій. Зростання обсягів електронного документообігу, поширення цифрових каналів зв’язку та ускладнення інформаційних потоків впливають на організацію режиму секретності та формують нові ризики для безпеки інформаційних ресурсів. Організаційні труднощі, кадрові проблеми, потреба оновлення технічної інфраструктури та вдосконалення процедур контролю за доступом до інформації визначають напрями розвитку системи захисту державної таємниці.

Удосконалення системи охорони державної таємниці охоплює модернізацію процедур обліку та зберігання секретної інформації, впровадження сучасних засобів кіберзахисту, підвищення рівня професійної підготовки персоналу та розвиток міжвідомчої координації. Використання цифрових технологій у сфері контролю за обігом інформації сприяє впорядкуванню режимних процедур та підтриманню стабільності функціонування системи секретності. Розвиток кадрового забезпечення, оновлення технічних засобів захисту та адаптація організаційних механізмів до сучасних інформаційних загроз впливають на здатність держави забезпечувати належний рівень захисту відомостей з обмеженим доступом.

ВИСНОВКИ

Охорона державної таємниці в Україні посідає значне місце у структурі забезпечення інформаційної безпеки держави та пов’язана із захистом відомостей, поширення яких може впливати на функціонування органів державної влади, оборонної сфери, зовнішньополітичної діяльності та інших напрямів державного управління. Формування системи захисту секретної інформації відбувається у межах загальної політики забезпечення національної безпеки, що охоплює організаційні, кадрові, технічні та правові механізми контролю за обігом інформації з обмеженим доступом. Розвиток сучасного інформаційного середовища супроводжується постійним збільшенням обсягів даних, що обробляються в електронних системах, використанням цифрових каналів зв’язку та інтеграцією інформаційних ресурсів у різні сфери державної діяльності.

Забезпечення охорони державної таємниці пов’язане з організацією режиму секретності, який охоплює порядок класифікації інформації, визначення рівнів доступу, ведення спеціального діловодства та контроль за використанням секретних матеріалів. Функціонування режиму секретності спрямоване на впорядкування процесів роботи з інформацією та визначення кола осіб, які мають право доступу до відомостей обмеженого доступу. Формування багаторівневої системи контролю за інформаційними потоками сприяє підтриманню цілісності системи захисту та зниженню ризиків несанкціонованого поширення інформації.

Охорона державної таємниці має значення для забезпечення стабільності діяльності державних інституцій та підтримання безпеки управлінських процесів. Інформація, що стосується оборонної сфери, функціонування систем безпеки, міжнародного співробітництва або стратегічних напрямів розвитку держави, потребує спеціального режиму захисту через можливі наслідки її розголошення. Контроль за доступом до таких відомостей спрямований на

збереження конфіденційності інформації та підтримання належного рівня безпеки у сфері державного управління.

Функціонування системи охорони державної таємниці пов’язане з діяльністю спеціально уповноважених органів, режимно-секретних підрозділів та посадових осіб, які забезпечують контроль за обігом інформації з обмеженим доступом. Організація їх роботи охоплює проведення перевірок, ведення обліку секретних документів, контроль за умовами зберігання інформації та дотриманням режимних вимог. Узгодженість дій між різними структурними елементами системи формує єдиний механізм захисту інформаційних ресурсів держави.

Розвиток цифрових технологій та поширення електронного документообігу впливають на структуру системи охорони державної таємниці та формують потребу у вдосконаленні технічних механізмів захисту інформації. Використання комп’ютерних мереж, електронних баз даних та цифрових каналів зв’язку супроводжується виникненням нових інформаційних загроз, пов’язаних із несанкціонованим доступом до даних, кібератаками та втручанням у роботу інформаційних систем. У зв’язку з цим значення технічного захисту інформації постійно зростає.

Охорона державної таємниці в Україні пов’язана із забезпеченням цілісності інформаційного простору держави та підтриманням безпеки стратегічних напрямів її діяльності. Функціонування системи захисту інформації охоплює організаційні, кадрові, технічні та управлінські механізми, що взаємодіють між собою у межах єдиної структури. Розвиток сучасних інформаційних технологій, зміна характеру інформаційних загроз та ускладнення цифрового середовища впливають на структуру режимних заходів і формують потребу у постійному вдосконаленні системи охорони державної таємниці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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

2. Ковальов К.Є., Леонов Б.Д. Забезпечення охорони державної та службової таємниці у сфері оперативно-розшукової діяльності за законодавством окремих держав: порівняль- ний 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

3. Пастернак М. С. Розмежування складів злочину, передбачених ст. 328 «Розголо- шення 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

4. 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

5. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. Редакція станом на 01.01.2026. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

6. 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

7. Кримінальний кодекс України: Кодекс України від 05.04.2001 р. № 2341-III. Редакція станом на 01.01.2026. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

8. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Редакція станом на 01.01.2026. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

9. 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

10. 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

11. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII. Редакція станом на 01.01.2026. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

12. 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

13. 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

14. 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

15. Постанова Кабінету Міністрів України № 939 від 18.12.2013 р. «Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях»: Постанова КМУ від 18.12.2013 р. № 939. Редакція станом на 01.01.2026. URL: https://zakon.rada.gov.ua/laws/show/939-2013-п#Text

16. 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

17. 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

18. 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

19. 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

20. 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

21. 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

22. 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.

23. 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

24. 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

25. 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

26. 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

27. 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

28. 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%BC%D0%B0%D0%BD%D0%B0%D1%85-2021-%D1%82%D0%B5%D0%BA%D1%81%D1%82.pdf#page=173

29. Берднік І. В., Головко 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

30. 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

31. 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

32. 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

33. 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

34. 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

35. 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

36. 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