МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ

Кафедра музеєзнавства, пам'яткознавства
та інформаційно-аналітичної діяльності

На правах рукопису

ЗІНЧУК МИКОЛА ВОЛОДИМИРОВИЧ

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УКРАЇНІ

Робота на здобуття освітнього ступеня «Бакалавр»
за освітньо-професійною програмою
«Документаційне забезпечення управління та інформаційно-аналітична діяльність»
Спеціальності 029 «Інформаційна, бібліотечна та архівна справа»

Науковий керівник:
кандидат історичних наук, доцент
Дмитренко А. А.

РЕКОМЕНДОВАНО ДО ЗАХИСТУ
Протокол № _____
засідання кафедри музеєзнавства,
пам'яткознавства та інформаційно-
аналітичної діяльності
від _____ 2024 р.
Завідувачка кафедри проф. Гаврилюк С. В._____

Луцьк – 2024

АНОТАЦІЯ

Зінчук М. В. Правове забезпечення захисту конфіденційної інформації в Україні. Кваліфікаційна робота на правах рукопису на здобуття освітнього ступеня «Бакалавр». Волинський національний університет імені Лесі Українки, Луцьк, 2024.

У дослідженні з'ясовано теоретичні аспекти захисту конфіденційної інформації, зокрема поняття та види конфіденційної інформації. Показано значення нормативно-правового регулювання у забезпеченні інформаційної безпеки, включаючи чинні закони та підзаконні акти, що регламентують цю сферу.

У першому розділі роботи проаналізовано правові механізми захисту конфіденційної інформації, що включають законодавчі, технічні та організаційні заходи. Здійснено детальний огляд існуючих нормативно-правових актів, що регулюють захист персональних даних, комерційної та державної таємниці в Україні.

У другому розділі висвітлені практичні аспекти забезпечення захисту конфіденційної інформації в Україні. Проаналізовано сучасні проблеми та виклики у сфері захисту конфіденційної інформації, наголошено на необхідності вдосконалення технічних та організаційних заходів для запобігання несанкціонованому доступу до конфіденційних даних. Доведено, що ефективний захист конфіденційної інформації вимагає інтегрованого підходу, який поєднує правові, технічні та організаційні засоби.

Наголошено на важливості міжнародної співпраці та адаптації кращих міжнародних практик для забезпечення високого рівня інформаційної безпеки в умовах швидкого розвитку інформаційних технологій та зростання кіберзагроз.

Ключові слова: конфіденційна інформація, інформаційна безпека, нормативно-правове регулювання, кіберзагрози, комерційна таємниця, правовий захист.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі, де інформація є одним із найважливіших активів, захист конфіденційної інформації стає все більш актуальним. В Україні, як і в багатьох інших країнах, існує ряд законодавчих актів та нормативних документів, які регулюють цю сферу. З розвитком інформаційних технологій і потужним прискоренням розвитку цифрового світу, кожного дня ми стикаємося не лише з новими можливостями для швидкого обміну даними, а й з новими викликами у забезпеченні приватності. У цьому контексті захист конфіденційної інформації стає особливо важливим у сучасному світі. Важливо враховувати, що Україна схожа на інші країни своїм досвідом активної цифрової трансформації. Це супроводжується широкомасштабним переходом до електронного зберігання та обробки інформації. В свою чергу це відкриває нові можливості для простого обміну даними, але водночас підвищує ризик порушення конфіденційності. Тому вивчення правового забезпечення захисту інформації є актуальним.

Метою дослідження є комплексний аналіз існуючої законодавчої та нормативно-правової бази України, що регулює захист конфіденційної інформації, який дозволить виявити сильні та слабкі сторони законодавства. Створення пропозицій щодо удосконалення правового регулювання, адаптація до сучасних викликів цифрової ери та підвищення ефективності захисту конфіденційної інформації в Україні.

Для досягнення мети дослідження поставлено такі **завдання**:

– детально проаналізувати чинні закони та нормативно-правові акти, що стосуються захисту конфіденційної інформації і дозволяють визначити їх ефективність та відповідність сучасним нормам;

– дослідити практику застосування правових принципів захисту інформації, включаючи аналіз судових справ та порушення інформаційної безпеки;

– охарактеризувати законодавства та практики інших країн щодо захисту конфіденційної інформації з метою визначення можливостей для вдосконалення системи українського законодавства;

– визначити основні проблеми та виклики, з якими стикаються суб’єкти, що здійснюють захист конфіденційної інформації в Україні;

– розробити рекомендації для удосконалення правового регулювання та практик захисту інформації, що включає в себе пропозиції щодо внесення змін до законодавства та поліпшення механізмів контролю;

– провести оцінку сучасних технологічних інструментів та методів захисту інформації та досліджено їх доступність та ефективність в українському контексті;

– визначити ключові напрямки розвитку системи захисту конфіденційної інформації в Україні на основі отриманих даних.

Об'єктом дослідження є система правових норм, яка регулює захист конфіденційної інформації, що включає правову основу, тобто Закони, статутні та нормативно-правові акти України, що визначають статус, доступ та вид захисту конфіденційної інформації.

Предметом дослідження є правова охорона конфіденційної інформації в Україні. Це включає в себе всі аспекти правових норм, які впливають на захист конфіденційної інформації в різних сферах діяльності, включаючи державний сектор, компанії, наукові установи та громадськість.

Стан наукової розробки проблеми характеризується активними дослідженнями та розробками в цій галузі, але все ще має багато невирішених проблем і викликів. В. Баскаков зазначає, що забезпечення захисту конфіденційної інформації є невід'ємною складовою інформаційної безпеки держави, і потребує чіткої регламентації та контролю з боку державних органів. Л. Борисова підкреслює важливість комплексного підходу до захисту конфіденційної інформації, включаючи технічні, організаційні та правові заходи. І. Гамбург зазначає, що ефективний захист комерційної таємниці є

важливим чинником конкурентоспроможності бізнесу. О. Кравченко у своїй роботі наголошує на необхідності вдосконалення правових механізмів та посилення контролю за дотриманням вимог щодо захисту конфіденційної інформації.

Для аналізу правового забезпечення захисту конфіденційної інформації в Україні було використано такі **методи**: нормативно-правовий аналіз, порівняльно-правовий метод, аналітичний метод, емпіричний метод та метод критичного аналізу.

Новизна одержаних результатів полягає у наступних факторах:

– виявлено та систематизовано проблемні аспекти у сфері захисту конфіденційної інформації в Україні, які включають слабкі місця в законодавстві, недоліки в застосовуваній практиці та інші фактори, що обмежують ефективність захисту даних;

– на основі отриманих результатів розроблено конкретні практичні рекомендації щодо вдосконалення правового регулювання та практики захисту секретної інформації в Україні;

– значну увагу приділено аналізу впливу нових технологій, таких як шифрування даних, блокчейн тощо, на захист конфіденційної інформації.

Практичне значення. Матеріали роботи можна використовувати для підвищення рівня інформаційної безпеки у державному та приватному секторах, а також у формуванні правової культури та захисту прав громадян. Використання результатів дослідження сприятиме підвищенню ефективності захисту конфіденційної інформації та забезпеченню стабільного розвитку інформаційного суспільства в Україні.

Апробація результатів дослідження. Основні положення кваліфікаційної роботи **доповідалися на** ІІІ Всеукраїнській науково-практичній конференції студентів та аспірантів «Україна у світовому просторі: минуле і сучасність» (м. Луцьк, 22 травня 2024 р.).

Публікація

Зінчук М. Практичні аспекти захисту конфіденційної інформації в Україні. *Україна у світовому просторі: минуле і сучасність* : збірник матеріалів ІІІ Всеукраїнської науково-практичної конференції студентів та аспірантів. Луцьк, 2024. С. 239–241.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ПРАВОВОГО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

1.1. Поняття та види конфіденційної інформації

У наш час інформація є одним із найцінніших ресурсів. Вона впливає на всі частини життя, від особистого до професійного, від економічного до політичного. Конфіденційна інформація потребує особливого захисту та регулювання серед різноманітних видів інформації. Визначення, класифікація та розуміння конфіденційної інформації є важливими для створення ефективних засобів її захисту.

Конфіденційна інформація стала важливим аспектом сучасного суспільства, де інформаційні ресурси відіграють ключову роль у діяльності державних органів, бізнесу та приватних осіб.

В умовах інформаційного суспільства захист конфіденційної інформації є важливим для безпеки країни, економічної стабільності та приватного життя кожного громадянина.

У цьому контексті виникає необхідність детального аналізу поняття та видів конфіденційної інформації, що є основою для подальшого правового регулювання та захисту.

Конфіденційна інформація – це будь-яка інформація, доступ до якої обмежується фізичною або юридичною особою, і яка не підлягає вільному поширенню через її особливу значимість або чутливість [2]. Така інформація може мати комерційну, особисту, професійну або державну цінність, і її розголошення може мати негативні наслідки для особи або для суспільства в цілому.

Відповідно до Закону України «Про інформацію» конфіденційна інформація визначається як інформація, доступ до якої обмежений фізичною або юридичною особою, за винятком органів державної влади, які виконують

свої повноваження. Це визначення підкреслює, що конфіденційні дані включають різноманітні дані, які можуть бути захищені різними правовими засобами.

Варто зазначити, що поняття конфіденційної інформації має динамічний характер і може змінюватися залежно від соціально-економічних умов, рівня розвитку інформаційних технологій та інших факторів [34].

Для захисту та правильного використання інформації важлива конфіденційність. Визначення та дотримання стандартів конфіденційності дозволяють ефективно захистити інформацію та запобігти її несанкціонованому використанню. Було розглянуто основні принципи конфіденційності інформації, що допоможуть зрозуміти, яку інформацію можна вважати конфіденційною та які заходи необхідно вживати для її захисту.

Інформація може вважатися конфіденційною, якщо вона відповідає кільком основним критеріям.

Доступ до конфіденційної інформації повинен бути **обмежений**. Це означає, що лише певне коло людей має право отримувати доступ до такої інформації. Багато різних механізмів можуть бути використані для обмеження доступу, наприклад:

– механізм контролю доступу, тобто використання систем контролю доступу, які обмежують доступ до інформації лише уповноваженим особам;

– механізм політики доступу, тобто створення внутрішніх правил і процедур, які визначають, хто і як може отримати доступ до конфіденційної інформації;

– механізм фізичного захисту, що означає захист інформації від неправомірного доступу за допомогою фізичних засобів, таких як сейфи, замки та охоронні системи [15].

Інформація є ключовим активом, який може мати значну вартість для її власника чи інших сторін, які мають до неї інтерес. Ця цінність може бути виражена у різних формах, залежно від контексту та сфери застосування.

Комерційна цінність відображається у важливості інформації для бізнес-середовища. Це можуть бути дані, які допомагають компаніям зберігати конкурентну перевагу, такі як бази даних клієнтів, фінансові звіти, маркетингові стратегії та ноу-хау виробництва. Така інформація є життєво важливою для успіху та розвитку підприємства.

Особиста цінність пов'язана з інформацією, яка стосується приватного життя людей. Це може включати в себе медичні записи, особисті ідентифікаційні дані, листування та інші особистісні дані, які люди бажають тримати у таємниці від сторонніх очей [3].

Державна цінність інформації проявляється у її значенні для національної безпеки та добробуту країни. Це можуть бути секретні дані, що стосуються оборонних технологій, економічних стратегій, а також інформація, яка використовується у міжнародних відносинах та дипломатії.

Забезпечення конфіденційності цієї інформації є критично важливим, оскільки її витік або несанкціонований доступ може призвести до значних фінансових втрат, порушення особистого життя або навіть загрози національній безпеці. Тому правове регулювання та захист такої інформації вимагає особливої уваги та вдосконалення відповідно до сучасних умов.

В Україні, правові обмеження доступу до конфіденційної інформації є ключовим елементом у захисті прав громадян та забезпеченні національної безпеки. Ці обмеження встановлені різними законодавчими актами, які регулюють використання та розповсюдження інформації, що має особливу вагу для особистого життя громадян, комерційної діяльності та державних інтересів [23].

Закон України «Про інформацію» визначає конфіденційну інформацію як таку, що стосується фізичної особи, а також іншу інформацію, доступ до якої обмежено. Закон «Про захист персональних даних» встановлює рамки для обробки та охорони особистих даних. Також, Закон України «Про державну таємницю» забезпечує захист інформації, яка має важливе значення для державної безпеки [34].

Відповідальність за порушення цих законів є суворою. Зокрема, стаття 182 Кримінального кодексу України передбачає покарання за незаконне збирання, зберігання, використання або поширення конфіденційної інформації без згоди особи.

Адміністративно-правовий режим в Україні встановлюється та регламентується нормами публічного права і має за мету охорону інтересів держави, фізичних і юридичних осіб. Цей режим використовує імперативний метод регулювання, що включає заборони та приписи, і забезпечується державним примусом.

Таким чином, правове регулювання конфіденційної інформації в Україні має комплексний характер і включає норми різних галузей права, що забезпечують захист інформації та відповідальність за її порушення. Це створює міцну основу для захисту конфіденційності та забезпечення прав громадян на недоторканість їхнього приватного життя [16].

Несанкціоноване розкриття конфіденційної інформації може мати серйозні наслідки як для суспільства загалом, так і для окремих осіб. Захист такої інформації є життєво важливим через потенційні збитки, які можуть виникнути в результаті такого розголошення.

Економічні наслідки можуть бути значними, включаючи зниження конкурентоспроможності компанії, фінансові збитки та знецінення її активів. Втрата комерційних секретів може призвести до зниження ринкової вартості компанії та збитків для акціонерів.

Порушення особистих прав можуть включати неправомірне використання персональних даних, порушення прав на приватність та інтелектуальну власність. Це може призвести до юридичних наслідків, а також до виплати збитків постраждалим особам.

Репутаційні втрати можуть бути невідновними, особливо в епоху соціальних медіа, де інформація поширюється миттєво. Погіршення іміджу компанії або особи може призвести до втрати довіри з боку клієнтів, партнерів та громадськості [13].

Загрози національній безпеці включають можливість витоку інформації, яка стосується стратегічних планів або оборони країни, і яка може призвести до дестабілізації політичної ситуації. Такі витоки можуть мати значні наслідки, такі як погіршення міжнародних відносин і національної безпеки.

Розробка ефективних методів захисту конфіденційної інформації залежить від визначення та оцінки потенційних ризиків. Це вимагає комплексного підходу, який включає як організаційні, так і технічні дії, а також постійне оновлення політик безпеки та навчання персоналу. На всіх рівнях управління необхідно пам'ятати про те, що збереження конфіденційності інформації є не тільки юридичним обов'язком, але й етичною потребою.

Комерційна таємниця є важливим аспектом діяльності будь-якого підприємства, оскільки вона охоплює конфіденційні дані, які є важливими для бізнесу, та які потрібно захистити від несанкціонованого доступу та розголошення.

Розуміння сутності комерційної таємниці, її правового регулювання та механізмів захисту є необхідним для ефективного управління інформаційними ресурсами підприємства.

Комерційна таємниця відіграє вирішальну роль у життєдіяльності сучасного бізнесу, становлячи невід'ємну частину його успіху та стабільності. Це інформація, яка містить в собі виробничі таємниці, фінансові дані, маркетингові стратегії, а також відомості про клієнтів та партнерів, що не доступна широкому колу осіб і має значну цінність для підприємства [13].

Важливість комерційної таємниці полягає у її здатності забезпечувати компанії переваги перед конкурентами, а також у захисті стратегічної інформації, яка може вплинути на ділову стратегію та розвиток підприємства. Інформація, що вважається комерційною таємницею, повинна бути конфіденційною, мати комерційну цінність та бути належним чином захищеною власником від неправомірного доступу та розголошення.

Порушення комерційної таємниці може призвести до цивільно-правової, адміністративної, а іноді й кримінальної відповідальності, що підкреслює серйозність таких дій. Тому ефективний захист комерційної таємниці є не лише юридичним обов'язком, але й стратегічною необхідністю для забезпечення стабільності та розвитку підприємства. Законодавче регулювання в Україні сприяє створенню безпечного інформаційного середовища та підтримує конкурентоспроможність національного бізнесу [13].

Професійна таємниця визначається як інформація, яку професіонал отримує в ході виконання своїх службових обов'язків і яка має конфіденційний характер. Така інформація не може бути розкрита або використана без явної згоди особи, яка її надала. Законодавство захищає цю інформацію, щоб забезпечити приватність, довіру та надійність у відносинах між клієнтом та професіоналом.

Медична таємниця стосується всієї інформації про здоров'я пацієнта, включаючи діагнози, лікування та медичну історію, яка є важливою для забезпечення якісної медичної допомоги.

Адвокатська таємниця охоплює інформацію, отриману адвокатом під час надання правових послуг, включаючи стратегії захисту та особисті дані клієнта, що вимагає строгої конфіденційності [29].

Нотаріальна таємниця включає в себе відомості, які нотаріус дізнається під час виконання нотаріальних дій, таких як оформлення документів та угод.

Журналістська таємниця захищає джерела інформації та матеріали, отримані журналістом для створення публікацій, якщо ці джерела бажають залишитися анонімними.

Банківська таємниця стосується інформації про банківські рахунки та фінансові операції клієнтів, яка вимагає нерозголошення з метою забезпечення фінансової безпеки.

Службова таємниця відноситься до інформації, яку службова особа отримує у процесі виконання своїх обов'язків, і яка не повинна бути

доступною публічно для забезпечення ефективності та безпеки службової діяльності [29].

Збереження професійної таємниці є ключовим для підтримання довіри між професіоналами та їхніми клієнтами, а також для забезпечення етичної та ефективної практики у різних сферах діяльності. Вона виступає як захист особистої інформації та сприяє створенню безпечного та конфіденційного середовища для обміну важливою інформацією.

Інформація, яка вважається професійною таємницею, має відповідати певним умовам. По-перше, вона повинна бути отримана в ході професійної діяльності, що означає, що фахівець здобуває її під час виконання своїх професійних завдань.

По-друге, інформація має бути конфіденційною, тобто не доступною для загального відома і відомою лише обмеженому колу осіб з законним правом на доступ. Для забезпечення цієї конфіденційності, професіонал повинен вживати заходів, таких як обмеження доступу, використання захищених систем та зберігання документів у безпечних місцях.

По-третє, інформація не може бути розкрита без згоди особи, яка її надала, і професіонал не має права її розголошувати або використовувати без ясної згоди, окрім випадків, коли це дозволено законом, наприклад, у ситуаціях, що становлять загрозу життю чи здоров’ю інших осіб, або для запобігання злочинам [26].

1.2. Нормативно-правове регулювання захисту конфіденційної інформації в Україні

В Україні захист конфіденційної інформації забезпечується комплексом законодавчих актів, які встановлюють правила інформаційної безпеки та норми правової охорони конфіденційних даних.

Конституція України, як верховний закон країни, визначає основоположні права та свободи громадян, серед яких ключове місце займає право на захист конфіденційної інформації. Аналізуючи статті Конституції, можна виділити ті, що безпосередньо чи опосередковано стосуються цього права [14].

Стаття 32 Конституції України гарантує кожному громадянину право на повагу до його особистого та сімейного життя, встановлюючи недопустимість будь-яких дій, що порушують конфіденційність особистої інформації без вираженої згоди особи. Це положення служить як основа для захисту особистих даних і приватності в українському законодавстві, забезпечуючи, що особиста інформація, включаючи дані про сімейний стан, здоров'я, освіту, фінансовий стан, не може бути предметом вільного обігу без дозволу власника.

Згідно з Конституцією, кожна особа має непорушне право на приватне життя, включаючи особисті та сімейні аспекти. Це право означає, що без згоди індивіда, жодна установа чи особа не може втручатися в його приватні справи, окрім ситуацій, які законодавство визначає як винятки. Таке положення служить захистом для даних, пов'язаних з особистими відносинами, станом здоров'я, особистими перевагами та іншими аспектами приватного життя.

Конституція України встановлює чіткі обмеження щодо обробки особистих даних, забороняючи будь-які дії, пов'язані зі збором, збереженням, використанням та розповсюдженням інформації, яка вважається конфіденційною, без отримання попередньої згоди від особи, до якої ця інформація належить. Це правило застосовується, якщо тільки закон не

передбачає іншого, забезпечуючи захист особистих прав громадян на приватність [14].

Кожен індивід має конституційне право бути поінформованим про особисті дані, які про нього зберігаються. Це охоплює знання про зібрані відомості, цілі їх використання та осіб, які мають до них доступ. Окрім того, існує можливість запитати корекцію або вилучення даних, якщо вони виявляться неточними або застарілими.

Окрім статті 32, що прямо стосується захисту конфіденційної інформації, в Конституції України є й інші статті, які впливають на цю сферу.

Конституція України в статті 31 висуває непорушне право кожної особи на конфіденційність у сфері особистого листування та інших форм комунікації, таких як телефонні розмови та телеграфна кореспонденція. Це положення має вирішальне значення для забезпечення захисту приватної інформації, що передається через ці канали [14].

Основа конфіденційності комунікацій полягає у забезпеченні права на приватне спілкування без страху незаконного втручання, такого як прослуховування або перехоплення повідомлень. Це право включає захист від будь-яких дій, які можуть порушити приватність особистих та сімейних розмов, листування, включаючи електронні комунікації.

Проте, Конституція також визнає, що існують певні обставини, за яких можливе обмеження цього права. Такі винятки можуть бути застосовані лише за рішенням суду та в строго визначених законом випадках, наприклад, у рамках кримінального розслідування або для захисту національної безпеки. Важливо, що будь-яке таке втручання має бути виправданим і не перевищувати межі, необхідні для досягнення законної мети [14].

У практичному застосуванні це означає, що правоохоронні органи та інші державні установи зобов’язані отримувати судовий дозвіл перед тим, як здійснювати будь-які дії, що втручаються у приватні комунікації громадян. Це забезпечує захист права на приватність та водночас дозволяє владі виконувати свої функції в рамках закону.

Стаття 34 Конституції України відкриває перед громадянами широкі можливості для вільного висловлення власних думок, поглядів та переконань. Це положення є одним із кутових каменів демократичного суспільства, дозволяючи кожному не лише формулювати власні ідеї, але й вільно їх обговорювати, розповсюджувати та обмінюватися ними з іншими.

Свобода думки та слова є запорукою прогресивного розвитку суспільства, оскільки вона сприяє відкритому діалогу, критичному мисленню та інноваціям. Вона дозволяє громадянам вільно висловлювати свої думки, навіть якщо вони суперечать офіційній позиції уряду чи інших інституцій, тим самим підтримуючи принципи демократії та плюралізму.

З іншого боку, право на збір та розповсюдження інформації має свої межі, які визначені законодавством для захисту конфіденційності, персональних даних та інших важливих аспектів суспільного життя. Це означає, що під час використання та поширення інформації необхідно поважати права інших осіб та дотримуватися встановлених законом обмежень [14].

Свобода вираження думок може бути обмежена в інтересах захисту прав інших людей, забезпечення національної безпеки, підтримання громадського порядку, охорони здоров’я населення та моральних цінностей. Такі обмеження мають бути чітко обґрунтовані та не можуть бути використані як засіб для невиправданого придушення дискусій або критики. Вони повинні бути справедливими та необхідними в демократичному суспільстві, що прагне до відкритості та прозорості.

Стаття 40 Конституції України відкриває перед громадянами можливість активної участі у державному управлінні через право на звернення. Це право дозволяє кожному індивіду або групі осіб висловлювати свої думки, ідеї, занепокоєння та пропозиції безпосередньо до органів влади, як на місцевому, так і на національному рівні.

Забезпечення конфіденційності звернень є обов’язком державних інституцій, що приймають та обробляють ці звернення. Це означає, що

особисті дані, викладені у зверненнях, повинні бути захищені від неправомірного розголошення, забезпечуючи тим самим довіру громадян до процесу звернення [14].

Посадові особи, які мають доступ до звернень, несуть відповідальність за збереження конфіденційності інформації, що міститься в них. Неправомірне розголошення такої інформації може підірвати довіру до державних структур та порушити права громадян, тому важливо дотримуватися високих стандартів конфіденційності та відповідальності.

Стаття 50 Конституції України відіграє важливу роль у забезпеченні екологічної безпеки та здоров'я громадян, проголошуючи право на безпечне довкілля. Згідно з цією статтею, кожен має право не лише на здорове довкілля, але й на компенсацію за шкоду, завдану порушенням цього права. Це стосується якості повітря, води, харчових продуктів та умов проживання, що безпосередньо впливають на добробут особи [14].

Право на інформацію про довкілля є ключовим аспектом цієї статті, оскільки воно надає громадянам можливість бути поінформованими про екологічні умови та потенційні ризики для здоров'я. Це право на інформацію включає доступ до даних про стан навколишнього середовища, якість продуктів харчування та предметів побуту, що дозволяє особам робити обґрунтовані вибори та вживати заходів для захисту власного здоров'я.

Однак, при наданні такої інформації, необхідно забезпечити захист конфіденційних даних. Інформація, яка може виявити особисті дані окремих осіб, повинна оброблятися з особливою обережністю, щоб не порушувати право на приватність, якщо інше не передбачено законодавством. Таким чином, стаття 50 підкреслює важливість збалансованого підходу до доступу до інформації та захисту персональних даних у контексті екологічної безпеки.

Стаття 59 Конституції України відіграє ключову роль у забезпеченні правосуддя, надаючи кожній особі невід'ємне право на отримання правової допомоги. Це право є фундаментальним для функціонування правової

держави, оскільки воно гарантує доступ до юридичних послуг та захисту прав і свобод громадян.

Адвокатська таємниця є одним з основних принципів правової професії, який зобов'язує адвокатів зберігати в таємниці інформацію, отриману від клієнтів під час надання правових послуг. Цей принцип є запорукою довіри між адвокатом і клієнтом, а також важливим елементом для забезпечення ефективності правової допомоги [14].

Захист прав клієнта в контексті адвокатської таємниці передбачає, що адвокати мають право не розкривати інформацію, яка становить таємницю, крім випадків, коли це дозволено або вимагається законом. Це положення сприяє захисту особистих інтересів клієнтів та підтримує принципи справедливості та недоторканності приватного життя.

Важливість статті 59 полягає також у тому, що вона встановлює основу для розвитку системи безоплатної правової допомоги, яка забезпечує доступ до юридичних послуг для осіб, які не мають змоги оплатити їх. Це сприяє рівності всіх перед законом та зміцнює правову систему країни. Таким чином, стаття 59 Конституції України є важливим інструментом для забезпечення правової захищеності громадян та підтримки демократичних засад суспільства [14].

Вищезазначені статті Конституції України мають значний вплив на захист конфіденційної інформації. Вони встановлюють основні принципи захисту таємниці комунікацій, свободи вираження, права на звернення, доступу до екологічної інформації та забезпечення правової допомоги. Ці положення створюють комплексну систему захисту конфіденційної інформації, яка є фундаментом для подальшого розвитку законодавства і забезпечення прав і свобод громадян в Україні.

Слід вказати, що конституційні положення України відіграють вирішальну роль у захисті конфіденційної інформації, створюючи правову основу для регулювання цієї важливої сфери. Вони визначають основні

принципи, які лежать в основі всього законодавства, що стосується збереження приватності та конфіденційності інформації [24].

Законодавча основа, закріплена в Конституції, вимагає, щоб усі нормативно-правові акти були узгоджені з її положеннями та не містили суперечностей. Це забезпечує єдність та послідовність у правовій системі країни.

Судова практика також базується на конституційних нормах, що гарантує захист прав громадян на конфіденційність у судових процесах. Суди використовують конституційні положення як критерій для оцінки законності дій, пов'язаних з обробкою конфіденційної інформації.

Органи державної влади та місцевого самоврядування також керуються конституційними принципами у своїй діяльності, що сприяє дотриманню прав на конфіденційність у виконанні адміністративних функцій [7].

Важливість конституційних положень полягає у тому, що вони не тільки формують правову основу для захисту конфіденційної інформації, але й сприяють розвитку законодавства, що відповідає сучасним вимогам інформаційного суспільства. Це створює міцний фундамент для забезпечення прав і свобод громадян, а також для розвитку правової культури, що базується на повазі до приватності та захисту персональних даних. Таким чином, конституційні положення є ключовими для забезпечення правової захищеності громадян та підтримки демократичних цінностей в Україні.

Цивільний кодекс України є фундаментальним документом, який визначає правові рамки для захисту конфіденційної інформації. Він встановлює правила, що регулюють статус, види та механізми захисту конфіденційних даних, забезпечуючи правову визначеність у цій сфері.

Цивільний кодекс України містить важливі положення, які стосуються прав та обов'язків осіб у сфері інформаційних відносин. Зокрема, він визначає інформацію як відомості, які можуть бути зафіксовані на матеріальних носіях або в електронній формі, включаючи конфіденційні дані. Кожна особа має право на доступ до інформації, необхідної для реалізації своїх прав і інтересів,

але це право має бути збалансоване з необхідністю захисту конфіденційності [38].

Кодекс визначає комерційну таємницю як інформацію з обмеженим доступом, яка має комерційну цінність і захищається власником. Суб'єкти господарювання мають право на захист своєї комерційної таємниці, а неправомірне її використання чи розголошення тягне за собою відповідальність.

Цивільний кодекс України також гарантує особисті немайнові права, включаючи право на недоторканність приватного життя та таємницю кореспонденції. Збирання та розповсюдження особистих даних без згоди особи є неприпустимим, крім випадків, визначених законом.

Цей кодекс передбачає відповідальність за шкоду, завдану порушенням прав на конфіденційну інформацію. Якщо особа завдає шкоди іншій особі через порушення її прав, вона зобов'язана відшкодувати заподіяну шкоду.

Він є ключовим інструментом у захисті конфіденційної інформації, забезпечуючи правову основу для регулювання цієї сфери та встановлюючи відповідальність за її порушення. Це сприяє створенню довіри та правової визначеності у відносинах, пов'язаних із конфіденційною інформацією, та підтримує принципи справедливості та прозорості у суспільстві [38].

Цивільний кодекс України відіграє важливу роль у регулюванні відносин, пов'язаних із захистом конфіденційної інформації. Він містить загальні положення про інформацію, визначає права на комерційну таємницю та особисту інформацію, встановлює відповідальність за порушення цих прав, а також визначає механізми захисту конфіденційної інформації. Він забезпечує правову основу для захисту конфіденційної інформації як у сфері приватних, так і в ділових відносин, сприяючи захисту прав і свобод фізичних та юридичних осіб в Україні.

Закон України «Про інформацію» є основним нормативно-правовим актом, що регулює правовідносини у сфері інформації. Цей законодавчий акт розкриває основні засади, якими керуються учасники інформаційних

відносин, встановлюючи правила для обробки та зберігання даних, а також надаючи особливий статус конфіденційній інформації.

Відповідно до закону, інформація вважається конфіденційною, якщо вона доступна лише вузькому колу осіб, має певну цінність, як комерційну, так і іншу, і її розголошення обмежене згодою власника. Таке визначення підкреслює важливість збереження конфіденційності в інформаційному просторі та необхідність відповідального ставлення до обігу інформації. Закон «Про інформацію» слугує основою для розробки детальніших правил та процедур, що забезпечують захист інформації від несанкціонованого доступу та використання, сприяючи тим самим створенню безпечного інформаційного середовища [34].

Закон України «Про захист персональних даних» встановлює правові рамки для забезпечення безпеки персональних даних громадян. Він визначає, що таке персональні дані, хто є суб'єктами та об'єктами цієї інформації, і яким чином ці дані повинні оброблятися, зберігатися та захищатися.

Закон накладає на власників даних відповідальність за їхній захист, вимагаючи від них вживати всіх необхідних заходів для запобігання неавторизованому доступу та зловживанню цією інформацією. Це створює правову основу для захисту інформаційної приватності осіб та сприяє створенню безпечного інформаційного середовища в країні [33].

Закон України «Про доступ до публічної інформації» відіграє важливу роль у забезпеченні прозорості та відкритості державного управління, надаючи громадянам право на доступ до інформації, яка перебуває у розпорядженні державних органів.

Цей закон підкреслює основоположні принципи відкритості та доступності інформації, одночасно враховуючи необхідність захисту інформації, що має конфіденційний характер, відноситься до службового використання або класифікується як державна таємниця.

Таким чином, закон встановлює баланс між правом громадян на інформацію та необхідністю забезпечення національної безпеки та захисту конфіденційних даних [30].

Закон України «Про державну таємницю» відіграє критичну роль у забезпеченні безпеки держави, встановлюючи чіткі правила для класифікації та охорони інформації, яка має стратегічне значення. Цей законодавчий акт визначає категорії інформації, що можуть бути віднесені до державної таємниці, та вимагає від усіх державних органів та їх співробітників дотримання високих стандартів безпеки при її обробці.

Особливий режим охорони державної таємниці передбачає комплекс заходів, які включають не тільки фізичний захист інформації, але й застосування сучасних технологій шифрування та інформаційної безпеки. Крім того, закон встановлює правові основи для притягнення до відповідальності осіб, які порушують режим таємності, забезпечуючи тим самим ефективний захист відомостей, важливих для національних інтересів України.

Можна дійти висновку, що Закон «Про державну таємницю» є ключовим елементом у системі національної безпеки, що підтримує стабільність та суверенітет держави [29].

Закон України «Про банки і банківську діяльність» слугує основою для регулювання банківської сфери, зокрема у питаннях конфіденційності. Він встановлює, що інформація про рахунки, фінансові операції та стан активів клієнтів є банківською таємницею, яка підлягає захисту.

Розкриття такої інформації дозволяється лише у визначених законом обставинах, що включає судові рішення та запити від правоохоронних органів, забезпечуючи тим самим баланс між приватністю клієнтів та вимогами законодавства [28].

Кримінальний кодекс України встановлює чіткі правила та наслідки для тих, хто порушує конфіденційність інформації. Він містить статті, які визначають кримінальну відповідальність за дії, що неправомірно порушують

приватність особи, такі як незаконне збирання чи розповсюдження особистих даних.

Однією з ключових статей є стаття 182, яка забороняє незаконне втручання в особисте життя громадян, включаючи неправомірне використання або розголошення конфіденційної інформації без згоди особи, до якої ця інформація належить. Це підкреслює серйозність, з якою держава ставиться до захисту права на приватність своїх громадян [20].

Господарський кодекс України служить надійним фундаментом для регулювання комерційних відносин, зокрема у питаннях, що стосуються конфіденційності.

Кодекс визначає правила, якими повинні керуватися суб'єкти господарювання для забезпечення належного захисту комерційної таємниці та іншої конфіденційної інформації. Він встановлює чіткі обов'язки для бізнес-структур щодо обробки та зберігання конфіденційних даних, а також передбачає відповідальність за їх неправомірне використання чи розголошення, що сприяє створенню довіри та забезпеченню прозорості в господарській діяльності.

Отже, Господарський кодекс України відіграє ключову роль у захисті комерційних інтересів та підтриманні конкурентного бізнес-середовища.

1.3. Правові механізми захисту конфіденційної інформації

Забезпечення конфіденційності інформації становить фундаментальну частину інформаційної безпеки в Україні. В епоху цифровізації, коли дані перетворюються на стратегічний актив, захист цієї інформації є критично важливим.

Державні установи, спецслужби та інші організації відіграють вирішальну роль у забезпеченні дотримання нормативно-правових актів, що регулюють цю сферу. Вони не тільки виконують наглядові функції, але й

активно діють для практичного захисту конфіденційних даних, включаючи особистісну інформацію, бізнес-секрети та інші форми конфіденційних даних.

Важливість такого захисту посилюється з ростом кіберзагроз та шахрайства, що вимагає від усіх секторів суспільства, від корпоративного до приватного, бути особливо пильними щодо збереження конфіденційності інформації.

Сучасні технології, такі як шифрування даних та багаторівневі системи аутентифікації, стають все більш важливими інструментами в арсеналі захисту інформації. Крім того, освітні програми та тренінги з підвищення обізнаності про інформаційну безпеку є ключовими для формування культури конфіденційності та захисту даних на всіх рівнях організацій [26].

Однією з ключових інституцій, відповідальних за захист конфіденційної інформації, є Уповноважений Верховної Ради України з прав людини (Омбудсмен). Ця посада була створена для забезпечення додержання конституційних прав і свобод людини та громадянина, а також для захисту прав на інформацію.

Основні функції та повноваження Омбудсмена:

– моніторинг дотримання прав на конфіденційність, тобто Уповноважений проводить систематичний моніторинг та аналіз законодавства, політик та практик, що стосуються захисту персональних даних. Він також здійснює перевірки діяльності органів влади та приватних компаній, щоб забезпечити їх відповідність встановленим нормам;

– Уповноважений приймає та розглядає скарги від громадян, які стверджують, що їх права на конфіденційність були порушені. Він може вимагати від організацій надання доказів та пояснень щодо їхніх дій;

– Уповноважений має право вносити подання до органів влади з метою усунення виявлених порушень. Він також може рекомендувати зміни до існуючого законодавства для покращення захисту конфіденційної інформації;

– Омбудсмен регулярно публікує звіти про стан дотримання прав на конфіденційність, організовує інформаційні кампанії та навчальні заходи для підвищення обізнаності громадян;

– Уповноважений співпрацює з міжнародними інституціями та організаціями для обміну досвідом та кращими практиками у сфері захисту конфіденційної інформації;

– Омбудсмен аналізує тенденції та виклики, пов'язані з конфіденційністю, та ініціює розробку нових законопроектів або поправок до існуючих законів;

– Уповноважений надає консультативну та юридичну підтримку особам, чиї права на конфіденційність були порушені, допомагаючи їм у відновленні своїх прав [4].

Ці обов'язки відображають важливість ролі Омбудсмена як ключового захисника прав на конфіденційність в Україні, особливо в контексті зростаючих кіберзагроз та швидкого розвитку цифрових технологій. Він не лише виступає як наглядач за дотриманням прав, але й як активний учасник у формуванні безпечного цифрового середовища для всіх громадян.

Не менш важливою інституцією у сфері захисту конфіденційної інформації є Державна служба спеціального зв'язку та захисту інформації України, відома як Держспецзв'язку, виступає ключовим елементом у системі національної безпеки, відповідаючи за реалізацію державної політики у сфері захисту інформації.

Як центральний орган виконавчої влади, Держспецзв'язку має широкий спектр обов'язків, спрямованих на забезпечення інформаційної безпеки країни.

Одним з основних завдань Держспецзв'язку є створення нормативно-правових актів, стандартів та методик, які визначають як має відбуватися захист інформації. Ця діяльність включає не лише розробку, але й впровадження цих документів, а також контроль за їх дотриманням [2].

Держспецзв’язку відіграє важливу роль у захисті державних інформаційних систем, особливо тих, що використовуються для електронного урядування, від різноманітних загроз, таких як несанкціонований доступ чи кібератаки.

Держспецзв’язку здійснює нагляд за станом технічного захисту інформації у різних державних структурах, забезпечуючи, щоб системи захисту відповідали встановленим стандартам. Це включає проведення аудитів та перевірок.

Для підтримки високого рівня компетентності у сфері технічного захисту інформації, Держспецзв’язку організовує навчання та сертифікацію спеціалістів, що забезпечує кваліфіковані кадри для виконання завдань із захисту інформації.

В умовах постійно зростаючих кіберзагроз, роль Держспецзв’язку стає все більш актуальною. Від її ефективності залежить не тільки безпека державних інформаційних ресурсів, але й захист конфіденційності громадян. Завдяки своїй роботі, Держспецзв’язку сприяє створенню надійного інформаційного простору, який є важливим для економічного розвитку та демократичного процесу в країні [2].

Національна поліція України та інші правоохоронні органи відіграють важливу роль у забезпеченні захисту конфіденційної інформації, зокрема, у боротьбі з кіберзлочинністю та іншими порушеннями у сфері інформаційної безпеки.

Правоохоронці ведуть розслідування інцидентів, що включають незаконний доступ до конфіденційних даних, їх крадіжку, розповсюдження чи інше неправомірне використання, забезпечуючи правопорядок у цифровому просторі.

Національна поліція тісно співпрацює з Держспецзв’язком, Омбудсманом та іншими органами, що займаються захистом конфіденційної інформації, обмінюючись важливою інформацією та координуючи спільні дії для протидії порушенням.

Правоохоронні органи проводять аналіз кіберзагроз, розробляють стратегії протидії та рекомендації для зміцнення інформаційної безпеки. Вони також займаються просвітницькою діяльністю, інформуючи громадян про потенційні загрози та методи захисту від них [2].

З огляду на швидкий розвиток технологій та зростання кіберзагроз, роль правоохоронних органів у захисті конфіденційної інформації є надзвичайно важливою.

Вони не тільки реагують на існуючі виклики, але й працюють над попередженням майбутніх загроз, забезпечуючи безпеку інформаційного простору України. Завдяки їхнім зусиллям, громадяни можуть відчувати себе захищеними від неправомірного втручання у їхнє приватне життя та збереження їхньої конфіденційності.

Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, відома як НКРЗІ, виконує ключову роль регулятора у сфері телекомунікацій та інформатизації, ставши важливим гравцем у захисті інформації, що передається через телекомунікаційні мережі [11].

НКРЗІ встановлює стандарти та вимоги для операторів зв'язку, щоб забезпечити технічний захист інформації. Вона регламентує процеси шифрування даних, захисту каналів зв'язку та обробки конфіденційної інформації, що є критично важливими для забезпечення безпеки інформаційного простору.

Комісія проводить перевірки та аудити, щоб забезпечити, що оператори зв'язку дотримуються встановлених стандартів захисту інформації, гарантуючи надійність та конфіденційність даних.

НКРЗІ також відповідає за розгляд скарг та звернень громадян, що стосуються порушення їхніх прав на конфіденційність у сфері зв'язку. Вона вживає необхідних заходів для усунення порушень та відновлення прав громадян.

Комісія стає все більш значущою у забезпеченні стійкості та безпеки інформаційних систем. Її робота сприяє не лише захисту даних, але й

підтримці довіри користувачів до телекомунікаційних послуг, що є фундаментальним для розвитку цифрової економіки та суспільства [11].

Завдяки регуляторній діяльності НКРЗІ, Україна може ефективно реагувати на постійно змінювані технологічні та інформаційні загрози, зміцнюючи свої позиції як країни з високим рівнем інформаційної безпеки.

Інституційні механізми захисту конфіденційної інформації в Україні є важливою складовою системи інформаційної безпеки держави. Вони включають діяльність державних органів, спеціальних служб та інших установ, які здійснюють контроль за дотриманням законодавства у сфері захисту інформації та забезпечують її збереження та цілісність. Кожна з інституцій виконує свої функції та має визначені повноваження, що дозволяє створити комплексну систему захисту конфіденційної інформації [11].

Ця система включає розробку та впровадження нормативно-правових актів, технічних засобів захисту, організаційних заходів, а також проведення навчання та підготовки персоналу. Взаємодія між різними органами та установами забезпечує ефективне реагування на загрози та порушення у сфері інформаційної безпеки, що сприяє захисту прав громадян та організацій на конфіденційність інформації.

Судовий захист конфіденційної інформації в Україні виступає як фундаментальний інструмент у забезпеченні особистих та корпоративних прав на приватність.

Система правосуддя країни пропонує механізми для відновлення прав, що були порушені, через судові позови, рішення про компенсацію збитків, та запровадження заходів для запобігання подальшим порушенням. Розвиток судової практики в цій області сприяє формуванню юридичних прецедентів та забезпечує ясність у застосуванні законів, що стосуються конфіденційності.

Громадяни та компанії мають право звертатися до суду для захисту своєї конфіденційної інформації. Судові позови можуть включати вимоги про зупинення порушень, компенсацію збитків, та інші дії, спрямовані на відновлення порушених прав [2].

Позови про припинення порушень конфіденційності дозволяють позивачам вимагати припинення незаконного розголошення або використання їхньої конфіденційної інформації. Суди можуть наказати відповідачам припинити такі дії та вжити необхідних заходів для забезпечення конфіденційності.

У випадках, коли права на конфіденційну інформацію були порушені, позивачі можуть вимагати відшкодування матеріальних збитків та компенсації за моральну шкоду.

Іноді позивачі можуть звертатися до суду з проханням офіційно визнати певну інформацію як конфіденційну, що є важливим для її подальшого захисту.

Ці судові процедури відіграють вирішальну роль у захисті прав на конфіденційність, дозволяючи особам ефективно захищати свої інтереси та відновлювати порушені права через правову систему [2].

Судовий захист конфіденційної інформації відіграє вирішальну роль у забезпеченні прав особи на приватність. Суди мають повноваження вживати забезпечувальні заходи для охорони такої інформації в ході судового розгляду, що дозволяє ефективно запобігати можливим порушенням.

Суди можуть накладати арешт на конфіденційну інформацію, яка перебуває у володінні відповідача чи третіх осіб, щоб унеможливити її незаконне використання або розповсюдження до завершення судового процесу. Такі дії забезпечують збереження інформації та захист прав позивача.

Суд може також встановити заборону на розповсюдження конфіденційної інформації до моменту винесення остаточного рішення, що служить додатковим захистом для позивача від неправомірних дій.

Крім того, суд може прийняти інші тимчасові заходи, які вважає за потрібне для захисту конфіденційної інформації, включаючи зобов’язання щодо знищення несанкціонованих копій інформації або повернення оригінальних документів.

Судова практика в Україні є ключовим елементом у визначенні меж конфіденційності інформації та уточненні застосування законів, що регулюють цю область. Вивчення рішень судів допомагає виявити тенденції, які формують правову базу для захисту конфіденційних даних [11].

Через аналіз судових рішень можна зрозуміти, як суди інтерпретують конфіденційність інформації, які критерії вони використовують для визначення порушень, та як вони оцінюють наслідки таких порушень.

Судові прецеденти відіграють важливу роль у формуванні юридичної практики, забезпечуючи однакове застосування законодавства. Вони служать джерелом правових орієнтирів для майбутніх справ.

Судова практика також висвітлює проблемні аспекти, такі як неоднозначність термінології, складнощі у доказуванні порушень, та труднощі, пов’язані з виконанням судових рішень.

Ці аспекти підкреслюють значення судової практики у захисті конфіденційної інформації, надаючи можливість для розвитку правових норм та забезпечення захисту прав громадян на приватність. Судові рішення не лише вирішують індивідуальні спори, але й сприяють розвитку загальних правових принципів у сфері конфіденційності.

Правові механізми захисту конфіденційної інформації в Україні є комплексом заходів, спрямованих на забезпечення збереження, цілісності та доступності конфіденційних даних.

Вони включають законодавчі, інституційні, технічні, організаційні та судові механізми, які разом створюють ефективну систему захисту конфіденційної інформації. Дотримання цих механізмів є необхідною умовою для забезпечення прав фізичних та юридичних осіб на конфіденційність та недоторканність приватного життя [15].

Комплексний підхід до захисту конфіденційної інформації, який включає законодавчі, інституційні, технічні, організаційні та судові механізми, є необхідним для ефективного забезпечення прав фізичних та юридичних осіб на конфіденційність. Важливою умовою є постійний

моніторинг та вдосконалення цих механізмів, врахування новітніх технологічних розробок, змін у законодавстві та розвитку судової практики.

Висновки. Проведене дослідження правового забезпечення захисту конфіденційної інформації в Україні висвітлило низку ключових аспектів, які формують сучасну систему захисту даних в країні.

Захист конфіденційної інформації є надзвичайно важливим для забезпечення прав фізичних та юридичних осіб на конфіденційність, збереження приватності та стабільності бізнесу. Розглянуті правові, інституційні, технічні та організаційні механізми дозволяють створити ефективну систему захисту конфіденційних даних, яка відповідає сучасним вимогам інформаційного суспільства.

Інституційні механізми захисту конфіденційної інформації включають діяльність державних органів, таких як Уповноважений Верховної Ради України з прав людини, Національна комісія з питань регулювання зв'язку та інформатизації та інші.

Отже, захист конфіденційної інформації в сучасному інформаційному суспільстві є критично важливим для забезпечення національної безпеки, економічної стабільності та приватного життя громадян. Конфіденційна інформація, яка включає комерційну, особисту та державну цінність, потребує особливого захисту через можливі негативні наслідки її розголошення. Основні принципи захисту конфіденційної інформації полягають в обмеженні доступу, використанні механізмів контролю доступу та фізичного захисту.

Основою правового захисту конфіденційної інформації в Україні є Конституція, яка гарантує права на приватність та захист особистих даних. Закони «Про інформацію», «Про захист персональних даних», «Про державну таємницю» та інші нормативно-правові акти забезпечують комплексний правовий захист конфіденційної інформації, визначаючи принципи, процедури та відповідальність за порушення режиму конфіденційності.

Якщо підсумувати вищезазначене, то можна дійти висновку, що ефективна система захисту конфіденційної інформації сприяє підвищенню

довіри громадян та бізнесу до державних і комерційних інституцій, збереженню приватності та національної безпеки. Важливим є постійний моніторинг та вдосконалення правових, технічних та організаційних механізмів захисту інформації з урахуванням новітніх технологічних розробок та змін у законодавстві. Це є ключовими факторами стабільного розвитку країни у цифрову епоху.

РОЗДІЛ 2
ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УКРАЇНІ

2.1. Проблеми та виклики у сфері захисту конфіденційної інформації

У сучасному світі, де інформаційні технології розвиваються з неймовірною швидкістю, питання захисту конфіденційної інформації стає все більш важливим. Україна, як і багато інших країн, стикається з серйозними викликами у цій сфері, особливо враховуючи зростаючу кількість кіберзагроз та хакерських атак. У цій статті ми розглянемо ключові проблеми, з якими зіштовхується Україна у забезпеченні безпеки конфіденційної інформації, та обговоримо можливі стратегії їх вирішення.

Застаріла правова основа є однією з головних перешкод на шляху ефективного захисту конфіденційної інформації в Україні. Чинне законодавство часто не встигає за швидкими змінами в технологічному світі, що призводить до виникнення правових вакуумів. Наприклад, існуючі закони можуть не враховувати особливості захисту даних у хмарних обчисленнях або при використанні технологій блокчейну.

Недостатнє регулювання новітніх технологій також створює значні ризики. Законодавство не завжди відображає реалії сучасного цифрового світу, де штучний інтелект та хмарні технології відіграють все більшу роль [8].

Невідповідність міжнародним стандартам є ще однією серйозною проблемою. Українське законодавство часто не відповідає вимогам міжнародних стандартів, таких як Загальний регламент захисту даних (GDPR), що ускладнює інтеграцію країни в глобальний інформаційний простір та створює додаткові виклики для захисту конфіденційної інформації.

Забезпечення конфіденційності інформації вимагає значних зусиль, особливо у фінансовому та кадровому аспектах. В контексті України, ці виклики набувають особливої актуальності через ряд факторів.

Обмеженість фінансових ресурсів ставить під загрозу можливість державних установ впроваджувати передові системи захисту інформації та забезпечувати адекватне навчання персоналу. Це створює прогалини в системі безпеки, які можуть бути використані зловмисниками [8].

Недостатність інвестицій у сфері кібербезпеки з боку приватного сектору, зокрема малих та середніх підприємств, є ще однією проблемою. Брак коштів для інвестування у захист інформації робить ці компанії особливо вразливими до кібератак.

Дефіцит кваліфікованих кадрів у галузі кібербезпеки є критичним. Недостатня кількість освітніх програм, що спеціалізуються на кібербезпеці, разом з еміграцією висококваліфікованих фахівців у пошуках кращих можливостей за кордоном, призводить до "відтоку мізків" та зниження рівня захисту інформації в країні.

У світі, де кібербезпека є критично важливою, застарілі технології становлять серйозну загрозу для захисту конфіденційної інформації. Ось деякі з основних проблем, пов'язаних з використанням застарілих систем:

– вразливості в застарілих технологіях – часто такі системи містять відомі слабкі місця, які хакери можуть експлуатувати, створюючи реальну загрозу для мережевої безпеки;

– брак оновлень та технічної підтримки – без регулярних оновлень безпеки від розробників, застарілі системи стають легкою мішенню для новітніх кібератак;

– труднощі з інтеграцією сучасних рішень – застарілі технології можуть ускладнювати впровадження новітніх систем безпеки, таких як інструменти для моніторингу та відповіді на інциденти, що є ключовими для захисту інформації [7].

Для підвищення рівня кібербезпеки, необхідно регулярно оновлювати програмне забезпечення та обладнання, а також забезпечувати їх сумісність з новітніми технологіями. Це дозволить створити більш надійну та ефективну систему захисту конфіденційної інформації.

Для ефективного захисту конфіденційної інформації критично важливою є координація дій та взаємодія між різними організаціями. Проте, в Україні існують певні перешкоди, які ускладнюють цей процес.

Першою проблемою є недоліки у координації між державними структурами, тобто часто відсутня єдина система координації, що ускладнює ефективне реагування на кіберзагрози та захист важливої інформації.

Наступною проблемою можна вважати обмежену взаємодія з бізнес-сектором, що означає що співпраця між урядовими органами та приватними компаніями не завжди налагоджена, що знижує загальну ефективність системи кібербезпеки [8].

Також слід згадати про проблеми з обміном інформацією, тобто недостатній обмін даними про кіберзагрози між організаціями ускладнює ідентифікацію та нейтралізацію потенційних загроз.

Захист конфіденційної інформації в Україні стикається з викликами, які вимагають інтеграції новітніх технологій та міжнародної співпраці. Новітні розробки, такі як штучний інтелектт та машинне навчання, можуть революціонізувати системи кібербезпеки, пропонуючи автоматизований аналіз даних та швидке реагування на загрози.

Однак, ці ж технології можуть бути використані зловмисниками для створення складних атак, наприклад, за допомогою «deepfake».

Інтернет речей (IoT) пропонує нові можливості для управління та автоматизації, але також відкриває двері для потенційних вразливостей через слабкі засоби захисту IoT-пристроїв. Хмарні технології надають зручність у зберіганні та обробці даних, але вимагають додаткових заходів безпеки, таких як шифрування та контроль доступу [8].

Технологія блокчейн забезпечує високий рівень безпеки, але її впровадження може бути складним через питання управління ключами та масштабованості.

Міжнародна співпраця є необхідною для ефективної боротьби з кіберзагрозами, які не обмежуються національними кордонами. Швидкий

обмін інформацією, узгодженість юридичних рамок, та вирівнювання рівня розвитку кібербезпеки між країнами є ключовими для успішної співпраці.

Політичні бар'єри, такі як розбіжності у національній безпеці та геополітичні інтереси, можуть ускладнювати цей процес, але їх подолання є важливим для створення ефективної глобальної системи кібербезпеки. Зусилля на міжнародному рівні, включаючи співпрацю та обмін знаннями, можуть значно підвищити рівень захисту конфіденційної інформації в Україні та інших країнах.

У сфері захисту конфіденційної інформації, законодавче регулювання відіграє ключову роль і має бути динамічним, щоб відповідати швидким змінам у технологіях та загрозах [9].

Гнучкість законодавства є необхідною для адаптації до нових викликів, включаючи розробку нових нормативних актів та оновлення існуючих. Відповідність міжнародним стандартам, як-от GDPR, забезпечує інтеграцію України у глобальний інформаційний простір та захист прав громадян. Забезпечення виконання законів через контроль та притягнення до відповідальності є критичним для ефективності законодавства.

Освіта та підготовка фахівців у сфері кібербезпеки забезпечують розуміння як юридичних, так і технічних аспектів захисту інформації.

Адаптація до нових загроз вимагає виявлення та аналізу нових кіберзагроз, використання передових технологій для захисту даних, та розробки нових методів захисту. Реагування на інциденти включає чіткий план дій, створення команд реагування на інциденти та проведення тренувань [9].

Аналіз та вдосконалення систем захисту після кожного інциденту є важливим для запобігання майбутнім атакам.

У сфері кібербезпеки, використання передових технологій є вирішальним для забезпечення надійного захисту конфіденційної інформації. Автоматизація процесів безпеки дозволяє оперативно ідентифікувати та реагувати на потенційні загрози, зменшуючи час відгуку на інциденти.

Шифрування даних є критичним компонентом у захисті інформації, як під час її зберігання, так і при передачі. Контроль доступу, особливо за допомогою багатофакторної аутентифікації, забезпечує додатковий рівень захисту від несанкціонованого доступу.

Системи виявлення та запобігання вторгненням (IDS/IPS) відіграють ключову роль у підтримці безпеки мережі, дозволяючи виявляти та блокувати атаки в реальному часі.

Інновації та дослідження у сфері кібербезпеки є життєво необхідними для розвитку нових методів захисту [9].

Інвестиції у дослідження та розробки сприяють створенню передових технологій, які можуть випереджати кіберзагрози. Співпраця з науковими установами відкриває доступ до останніх наукових знахідок та інновацій у галузі.

Тестування та оцінка систем безпеки допомагають виявляти слабкі місця та вдосконалювати заходи захисту. Впровадження інноваційних рішень, таких як блокчейн та квантове шифрування, може значно підвищити рівень безпеки інформації, забезпечуючи її надійний захист від сучасних загроз.

Ці кроки є важливими для створення міцної та адаптивної системи кібербезпеки, здатної протистояти постійно еволюціонуючим кіберзагрозам [18].

Захист конфіденційної інформації є однією з найважливіших задач у сучасному інформаційному суспільстві. В Україні існує ряд проблем та викликів у цій сфері, які потребують комплексного підходу до вирішення.

Вдосконалення правової бази, підвищення рівня фінансування, навчання та підвищення обізнаності, використання сучасних технологій та міжнародна співпраця є ключовими елементами для забезпечення ефективного захисту конфіденційної інформації. Впровадження цих заходів дозволить не тільки підвищити рівень безпеки, але й забезпечити стабільний розвиток інформаційного суспільства в Україні.

2.2. Заходи щодо захисту інформації від несанкціонованого доступу

Заходи щодо захисту інформації від несанкціонованого доступу можна розділити на кілька основних категорій: фізичні, адміністративні, технічні та організаційні. Кожна з цих категорій має свої особливості та сфери застосування.

Фізичні заходи безпеки відіграють важливу роль у захисті конфіденційної інформації, обмежуючи доступ до критичних приміщень та обладнання. Контроль доступу до приміщень за допомогою магнітних карток, біометричних сканерів та кодових замків є ефективним способом забезпечення доступу лише уповноваженим особам.

Відеоспостереження допомагає відстежувати активність у приміщеннях та швидко реагувати на будь-які підозрілі дії. Сейфи та шафи для зберігання надають додатковий рівень фізичного захисту для паперових документів та носіїв інформації. Нарешті, охорона грає ключову роль у фізичному захисті приміщень, забезпечуючи безпеку майна та інформації.

Для підвищення ефективності фізичних заходів безпеки, можна впровадити додаткові технології та процедури, такі як системи раннього виявлення вторгнення, посилення структурної безпеки приміщень, та регулярне проведення тренувань з реагування на надзвичайні ситуації.

Також важливо регулярно переглядати та оновлювати плани безпеки, щоб вони відповідали сучасним загрозам та стандартам. Ці кроки допоможуть створити більш надійну та міцну систему фізичного захисту конфіденційної інформації від несанкціонованого доступу [9].

Адміністративні заходи захисту є фундаментальною частиною стратегії інформаційної безпеки, яка включає набір політик, процедур та правил. Ці заходи визначають, як організації повинні управляти доступом до інформації та її використанням.

Політики інформаційної безпеки встановлюють стандарти для зберігання, обробки та передачі даних. Процедури управління доступом

забезпечують, що лише уповноважені особи мають доступ до конфіденційної інформації. Навчання та тренінги сприяють підвищенню обізнаності працівників з питань безпеки та важливості захисту даних. Контроль та аудит допомагають переконатися, що політики та процедури дотримуються належним чином.

Для підсилення адміністративних заходів захисту, можна впровадити додаткові ініціативи, такі як розробка детальних планів реагування на інциденти, створення спеціалізованих команд з реагування на інциденти, та проведення регулярних внутрішніх та зовнішніх аудитів систем безпеки.

Також важливою є розробка програми постійного професійного розвитку для фахівців у сфері інформаційної безпеки, щоб вони могли залишатися в курсі останніх тенденцій та кращих практик у галузі.

Технічні заходи захисту є невід’ємною частиною комплексної системи кібербезпеки, яка використовує апаратні та програмні засоби для забезпечення безпеки інформації. Ось деякі з ключових технічних заходів [8].

Шифрування даних є основоположним інструментом для захисту конфіденційності інформації, який застосовується як для даних, що зберігаються, так і для даних, що передаються, запобігаючи несанкціонованому доступу у випадку їх перехоплення.

Антивірусні програми та фаєрволи відіграють важливу роль у захисті комп’ютерних систем від шкідливого програмного забезпечення та несанкціонованого доступу, створюючи бар’єр проти потенційних загроз.

Системи виявлення та запобігання вторгненням (IDS/IPS) дозволяють виявляти та блокувати спроби несанкціонованого доступу до мережі, забезпечуючи додатковий рівень захисту.

Контроль доступу до мережі через засоби, такі як VPN та багатофакторна аутентифікація, забезпечує безпечний доступ до інформаційних ресурсів, обмежуючи можливість несанкціонованого втручання [10].

Для посилення технічних заходів захисту, можна впровадити додаткові інструменти, такі як системи захисту від витоку даних (DLP), розширені системи аналітики поведінки користувачів та ендпойнтів, а також використовувати криптографічні протоколи нового покоління для забезпечення високого рівня шифрування.

Регулярне оновлення програмного забезпечення та апаратних компонентів, а також проведення пенетраційних тестів та вразливостей, допоможуть забезпечити актуальність та ефективність технічних заходів захисту.

Організаційні заходи захисту є важливою складовою загальної стратегії інформаційної безпеки, оскільки вони стосуються управління людськими ресурсами та формування культури, яка підтримує безпеку інформації. Вони включають:

– розподіл обов’язків – це забезпечує, що жоден працівник не має надмірного доступу до інформації, що мінімізує ризики зловживань та витоку даних;

– класифікація даних – встановлення різних рівнів доступу до інформації згідно з роллю працівника в організації, що дозволяє обмежити доступ до найбільш чутливої інформації;

– моніторинг та звітність – використання систем моніторингу для відстеження активності користувачів та звітність для аналізу та реагування на можливі порушення політик безпеки;

– управління інцидентами – розробка процедур для ефективного реагування на інциденти, включаючи швидке виявлення, зупинення атаки та відновлення операцій після інцидентів [10].

Для зміцнення організаційних заходів захисту, можна впровадити регулярні оцінки ризиків, розробити програми постійного навчання та свідомості з питань безпеки для всіх працівників, та створити спеціалізовані команди з безпеки, які займатимуться питаннями відповідності та реагування

на інциденти. Також важливою є інтеграція етичних стандартів та політик конфіденційності в корпоративну культуру, щоб підтримувати високий рівень відповідальності та прозорості в управлінні інформацією.

Захист інформації від несанкціонованого доступу є надзвичайно важливим завданням для будь-якої організації. Для забезпечення ефективного захисту необхідно впроваджувати комплексні заходи, що включають фізичні, адміністративні, технічні та організаційні заходи.

Інтеграція цих заходів у єдину систему захисту, постійне вдосконалення та підтримка з боку керівництва дозволяють значно підвищити рівень безпеки інформації та мінімізувати ризики несанкціонованого доступу.

2.3. Шляхи вдосконалення правового забезпечення захисту конфіденційної інформації

Удосконалення правового регулювання захисту конфіденційної інформації в Україні вимагає гармонізації з міжнародними стандартами та впровадження нових норм. Це передбачає прийняття законодавчих актів, що відповідають таким стандартам, як GDPR, з метою:

– встановлення ключових принципів захисту даних – розробка принципів обробки персональних даних, які забезпечують їх законне, справедливе та прозоре використання, з урахуванням необхідності обмеження зберігання та гарантування їх цілісності та конфіденційності;

– зміцнення прав суб’єктів даних – гарантування прав осіб на доступ до їхніх даних, можливість їх виправлення, видалення, а також обмеження обробки та перенесення даних;

– визначення обов’язків для контролерів та операторів даних – встановлення чітких вимог до контролерів та операторів даних щодо забезпечення безпеки персональних даних, включаючи обов’язок інформування про порушення безпеки даних, проведення оцінок впливу на захист даних та призначення відповідальних за захист даних [13].

Україна прагне зміцнити захист персональних даних, що вимагає оновлення законодавства для відповідності сучасним стандартам. Організації мають нести відповідальність за інформування про витоки даних у короткі терміни для оперативного реагування.

Проведення оцінки впливу на захист даних перед запуском ризикованих процесів допоможе мінімізувати потенційні загрози. Важливою є наявність уповноважених осіб з захисту даних у кожній організації, які забезпечують дотримання політик безпеки та ефективне реагування на інциденти.

Такі кроки сприятимуть підвищенню рівня захисту даних в Україні, забезпечуючи їх відповідність до міжнародних вимог і зміцнення довіри до цифрової економіки країни.

Україна, прагнучи до зміцнення захисту персональних даних, має взяти курс на активну співпрацю з міжнародними організаціями у сфері кібербезпеки. Це передбачає не лише обмін досвідом та кращими практиками через участь у міжнародних заходах, але й участь у спільних проектах, які сприятимуть підвищенню рівня захисту даних. Отримання консультацій та підтримки від цих організацій допоможе Україні у вдосконаленні національного законодавства у сфері захисту даних [13].

Ключовим елементом у цьому процесі є також регулярний перегляд та оновлення законодавчих актів, щоб вони відповідали новітнім технологічним розробкам та викликам. Моніторинг нових технологій та викликів, залучення фахівців для оцінки та вдосконалення нормативної бази, а також проведення публічних консультацій з громадськістю та бізнесом є важливими для створення ефективного та актуального правового поля.

Зміцнення захисту даних в Україні вимагає комплексного підходу, який поєднує міжнародну співпрацю, оновлення законодавства, інвестиції в технології та освіту. Все це сприятиме створенню надійної системи захисту персональних даних, яка зможе адекватно реагувати на сучасні виклики та забезпечити безпеку інформації в цифрову епоху.

У відповідь на стрімкий розвиток технологій, Україна прагне адаптувати своє законодавство, щоб воно відображало специфіку сучасних інновацій, таких як штучний інтелект, блокчейн та Інтернет речей [10].

Регулювання штучного інтелекту має забезпечувати прозорість та відповідальність у його застосуванні, особливо при обробці персональних даних. З огляду на блокчейн, законодавство має враховувати його децентралізовану природу та незмінність записів, що вимагає особливого підходу до регулювання. Щодо Інтернету речей, необхідно встановити чіткі вимоги до безпеки та конфіденційності даних, які ці пристрої збирають та передають, забезпечуючи захист від несанкціонованого доступу та зловживань.

В Україні потрібно розробляти спеціалізовані законів, які регулюватимуть використання новітніх технологій. Це передбачатиме створення правових рамок для хмарних сервісів, що включатимуть вимоги до шифрування та управління доступом до даних, забезпечуючи їх безпеку та конфіденційність.

Також необхідно встановити стандарти захисту даних на мобільних пристроях, використовуючи сучасні засоби шифрування та аутентифікації. Важливим аспектом є регулювання систем Інтернету речей, де потрібно врахувати вимоги до безпеки, щоб запобігти кібератакам та несанкціонованому доступу.

Забезпечення ефективного захисту конфіденційної інформації в Україні вимагає впровадження комплексного підходу, який об’єднує різні рівні управління та контролю. Центральним елементом цього підходу є створення національної комісії з кібербезпеки, яка координуватиме дії усіх зацікавлених сторін, розроблятиме стратегії та політики, а також здійснюватиме моніторинг їх виконання [13].

Також критично важливою є координація між різними державними органами, що забезпечить узгодженість дій та ефективний обмін інформацією, необхідним для реагування на сучасні виклики у сфері кібербезпеки.

Україна активно працює над створенням національної стратегії з кібербезпеки, яка охоплює комплексні заходи для захисту конфіденційної інформації. Ця стратегія передбачає чітке визначення ключових напрямків та завдань, що мають найвищий пріоритет у сфері безпеки даних. Розроблені плани дій мають на меті не лише підвищити рівень захисту інформації, але й забезпечити її відповідність до міжнародних стандартів.

Важливою складовою стратегії є система моніторингу та оцінки, яка дозволяє вчасно ідентифікувати слабкі місця та вносити необхідні корективи для забезпечення ефективного захисту в динамічному цифровому середовищі.

Слід наголосити, що в Україні активно запроваджуються системи управління інформаційною безпекою, що відповідають міжнародним стандартам ISO/IEC 27001 [8].

Цей процес охоплює комплексні кроки, починаючи з оцінки ризиків, яка дозволяє ідентифікувати потенційні загрози та вразливості. На основі цієї оцінки розробляються та впроваджуються політики та процедури, які спрямовані на ефективне управління ризиками та забезпечення надійного захисту даних. Для забезпечення актуальності та ефективності системи, вона постійно моніториться та удосконалюється, щоб відповідати змінам у сфері кібербезпеки та технологій.

Для забезпечення дотримання законодавства в сфері захисту конфіденційної інформації, Україна розгортає систему моніторингу та аудиту. Ця система передбачає проведення регулярних перевірок, щоб забезпечити відповідність діяльності організацій встановленим нормам.

Оцінка відповідності допомагає визначити, наскільки ефективно організації виконують вимоги законодавства. Встановлення системи звітування про результати перевірок та аудитів є ключовим для виявлення порушень та оперативного вжиття коригувальних заходів. Такий підхід сприяє підвищенню рівня правової відповідальності та зміцненню захисту інформації в країні.

Задля зміцнення законодавчого захисту конфіденційної інформації, потрібне введення більш жорстких санкцій за їх порушення. Значні фінансові штрафи мають бути встановлені для тих, хто порушує вимоги законодавства у цій сфері [9].

Крім того, адміністративна відповідальність має бути запроваджена для керівників організацій, які не дотримуються законних норм. У випадках серйозних порушень, таких як несанкціонований доступ або неправомірне використання конфіденційної інформації, має бути передбачена кримінальна відповідальність.

Ці заходи спрямовані на посилення правових гарантій та створення ефективної системи запобігання та реагування на порушення у сфері інформаційної безпеки.

Вдосконалення правового забезпечення захисту конфіденційної інформації в Україні є надзвичайно важливим завданням, яке потребує комплексного підходу.

Адаптація законодавства до міжнародних стандартів, оновлення та модернізація нормативних актів, впровадження комплексного підходу та забезпечення виконання законів дозволять значно підвищити рівень захисту конфіденційної інформації та забезпечити стабільний розвиток інформаційного суспільства в Україні.

Лише через спільні зусилля держави, приватного сектору та громадянського суспільства можна створити ефективну систему захисту конфіденційної інформації, яка відповідатиме сучасним викликам та забезпечить безпеку національних інформаційних ресурсів.

Висновки. На основі проведеного дослідження правового забезпечення захисту конфіденційної інформації в Україні можна зробити низку важливих висновків, які охоплюють теоретичні та практичні аспекти цієї проблеми.

В Україні існує ряд законодавчих проблем, які суттєво ускладнюють ефективний захист конфіденційної інформації. Серед них найбільш критичними є застарілість правової бази та невідповідність міжнародним

стандартам. Чинне законодавство не завжди встигає за швидкими змінами в технологічному світі, що призводить до правових вакуумів та недостатнього регулювання новітніх технологій, таких як штучний інтелект та хмарні обчислення.

Недостатнє регулювання новітніх технологій створює значні ризики для захисту конфіденційної інформації. Законодавство не завжди відображає реалії сучасного цифрового світу, що призводить до невідповідності міжнародним стандартам, зокрема Загальному регламенту захисту даних (GDPR). Це ускладнює інтеграцію України в глобальний інформаційний простір та створює додаткові виклики для захисту конфіденційної інформації.

Забезпечення конфіденційності інформації вимагає значних зусиль, особливо у фінансовому та кадровому аспектах. В Україні ці виклики набувають особливої актуальності через обмеженість фінансових ресурсів та недостатність інвестицій у сфері кібербезпеки з боку приватного сектора. Це призводить до нестачі сучасних систем захисту інформації та недостатнього навчання персоналу, що створює прогалини в системі безпеки.

Одним із шляхів вирішення проблеми є гармонізація національного законодавства з міжнародними стандартами та посилення міжнародної співпраці. Впровадження міжнародного досвіду та стандартів допоможе підвищити ефективність захисту конфіденційної інформації в Україні та сприятиме інтеграції країни в глобальний інформаційний простір.

Сучасні технології можуть суттєво підвищити рівень захисту конфіденційної інформації. Впровадження передових технологічних рішень, таких як криптографія, біометрична аутентифікація та системи штучного інтелекту, дозволить значно зміцнити інформаційну безпеку. Особливо важливим є розвиток технологій для захисту даних у хмарних обчисленнях, які все більше використовуються в сучасному світі.

Не менш важливим є навчання та підвищення кваліфікації фахівців у сфері кібербезпеки. Регулярне проведення тренінгів, семінарів та курсів з інформаційної безпеки дозволить забезпечити високий рівень підготовки

кадрів, що, в свою чергу, позитивно вплине на загальний рівень захисту конфіденційної інформації.

Для ефективного захисту конфіденційної інформації необхідна активна підтримка з боку держави. Це включає не лише оновлення законодавчої бази, але й надання фінансової підтримки для впровадження сучасних технологій та навчання фахівців. Розробка державних програм з кібербезпеки та залучення інвестицій у цю сферу є критично важливими для досягнення високого рівня інформаційної безпеки.

Регулярний моніторинг та аудит систем захисту конфіденційної інформації дозволить своєчасно виявляти та усувати вразливості. Впровадження системи незалежного аудиту забезпечить об'єктивну оцінку стану інформаційної безпеки та сприятиме постійному вдосконаленню захисних заходів.

Враховуючи наведені висновки, стає очевидним, що питання захисту конфіденційної інформації в Україні є надзвичайно актуальним та багатогранним. Ефективне вирішення цієї проблеми вимагає комплексного підходу, який включає оновлення законодавчої бази, впровадження сучасних технологій, підвищення кваліфікації фахівців та активну підтримку з боку держави. Лише за умови реалізації всіх зазначених заходів можна досягти високого рівня захисту конфіденційної інформації та забезпечити інформаційну безпеку країни в сучасному цифровому світі.

ВИСНОВКИ

У ході проведеного дослідження правового забезпечення захисту конфіденційної інформації в Україні було розглянуто ряд проблем та шляхів для подальшого їх вирішення.

З'ясовано, що захист конфіденційної інформації є однією з ключових задач сучасного інформаційного суспільства. В умовах швидкого розвитку інформаційних технологій та зростання кількості кіберзагроз, особливої важливості набуває правове регулювання та ефективне управління інформаційною безпекою.

Перш за все, конфіденційна інформація включає дані, доступ до яких обмежується фізичними або юридичними особами через їх особливу значимість або чутливість. Вона може мати комерційну, особисту, професійну або державну цінність. Закон України «Про інформацію», «Про захист персональних даних» та інші нормативно-правові акти створюють основу для захисту конфіденційної інформації, визначаючи правила обробки, зберігання та розповсюдження даних.

Захист цієї інформації є критично важливим для національної безпеки, економічної стабільності та приватного життя громадян. Забезпечення надійного захисту конфіденційної інформації в Україні є важливим кроком до створення правової держави та інформаційного суспільства.

Україна стикається з рядом проблем та викликів у сфері захисту конфіденційної інформації, які вимагають негайного вирішення. Однією з ключових проблем є застаріле законодавство, яке не встигає за швидкими змінами в технологічному світі, створюючи правові вакууми та відкриваючи шлях для потенційних загроз.

Крім того, обмежені фінансові ресурси та дефіцит кваліфікованих фахівців у сфері кібербезпеки ускладнюють розробку та впровадження ефективних заходів захисту. Технологічні виклики, такі як використання застарілих систем та недостатня інтеграція новітніх технологій, послаблюють

захист даних, підвищуючи ризики витоку та несанкціонованого доступу до конфіденційної інформації.

Ці проблеми вимагають комплексного підходу, який включає оновлення законодавства, збільшення інвестицій у сферу кібербезпеки та розвиток кадрового потенціалу, а також ширше впровадження та адаптацію до сучасних технологій.

Звичайно, слід наголосити на тому, що для підвищення рівня захисту конфіденційної інформації, Україна вживає низку заходів, що охоплюють фізичні, адміністративні, технічні та організаційні аспекти.

Фізичні заходи включають в себе контроль доступу до приміщень, відеоспостереження, використання сейфів для зберігання важливих документів та забезпечення фізичної охорони для запобігання несанкціонованому доступу.

Адміністративні заходи полягають у розробці та впровадженні внутрішніх політик та процедур, що регулюють обробку та зберігання інформації, а також у навчанні персоналу з питань інформаційної безпеки. Моніторинг дотримання цих норм є ключовим для підтримання високого рівня захисту.

Технічні заходи включають використання шифрування для захисту даних, багаторівневої аутентифікації для підтвердження ідентичності користувачів та систем виявлення та запобігання вторгненням, які допомагають виявляти та блокувати потенційні загрози.

Організаційні заходи передбачають координацію дій між різними державними та приватними структурами, а також міжнародну співпрацю для обміну досвідом та кращими практиками у сфері кібербезпеки. Ці комплексні дії спрямовані на створення ефективної системи захисту, яка зможе протистояти сучасним викликам у сфері інформаційної безпеки.

Узагальнюючи, захист конфіденційної інформації в Україні потребує комплексного підходу, який включає вдосконалення правової бази,

підвищення фінансування та рівня обізнаності, використання сучасних технологій та активну міжнародну співпрацю.

Ефективна система захисту даних сприяє підвищенню довіри громадян та бізнесу до державних і комерційних інституцій, збереженню приватності та національної безпеки, що є ключовими факторами стабільного розвитку країни у цифрову епоху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Актуальні проблеми правоохоронної діяльності : матеріали Міжнародної науково-практичної конференції (м. Київ, 20 грудня 2010 року) / В. Ліпкан (голова редкол.); відповідальні за випуск: Баскаков В. Київ: 2010. С. 59–61.

2. Борисова Л. В. Правові засади захисту інформації: навч. посіб. Харків: ХНУВС, 2013. 212 с.

3. Бундз Р. О. Захист конфіденційної інформації: наукові записки Львівського університету бізнесу та права. Львів, 2022. С. 177–182. URL: https://nzlubp.org.ua/index.php/journal/article/view/651/596 (дата звернення: 11.04.2024).

4. Гамбург І. А. Правове забезпечення захисту комерційної таємниці в Україні. *Держава та регіони. Серія: Право*. 2011. № 2. С. 64–69.

5. Гордієнко С. Г. Конфіденційна інформація та «таємниці»: їх співвідношення. *Часопис Київського університету права*. 2013. № 4. С. 233–238.

6. Дідук А. Г. Правовий режим інформації, конфіденційної інформації. *Науковий вісник Ужгородського національного університету. Серія: Право.* Ужгород, 2013. С. 142–145. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/16424 (дата зверненян: 11.04.2024).

7. Дідук А. Г. Щодо деяких аспектів правової охорони конфіденційної інформації в Україні. *Наше право.* 2013. № 9. С. 152–159.

8. Завертнева-Ярошенко В. А. Проблеми правового захисту комерційної таємниці в Україні. *Правова держава*. 2018. № 32. С. 134–145. URL: http://nbuv.gov.ua/UJRN/Prav_2018_32_17 (дата звернення: 10.04.2024).

9. Захист конфіденційної інформації – персональних даних. URL: http://surl.li/uiygh (дата звернення: 9.04.2024).

10. Захист персональних даних. URL: https://wiki.legalaid.gov.ua/index.php/%D0%97%D0%B0%D1%85%D0%B8%D1

%81%D1%82_%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85 (дата звернення: 12.05.2024).

11. Іванців Я. І. Правовий захист комерційної таємниці. URL: https://ukrainepravo.com/scientific-thought/pravova-pozytsiya/pravoviy-zakhist-komerts-yno-ta-mnits/ (дата звернення: 11.05.2024).

12. Інформаційні стратегії в глобальному управлінні : матеріали Міжнародної науково-практичної конференції (м. Київ, 29 жовтня 2011 року) / В. Ліпкан (голова редкол.); відповідальні за випуск: Баскаков В. Київ: 2011. С. 47–51.

13. Комерційна таємниця: інструменти захисту та відповідальність за розголошення. URL: https://biz.ligazakon.net/analitycs/214258_komertsyna-tamnitsya-nstrumenti-zakhistu-ta-vdpovdalnst-za-rozgoloshennya (дата звернення: 14.04.2024).

14. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.

15. Кормич Б. А. Інформаційне право : навч. посіб. для вищ. навч. закл. Харків : БУРУН і К, 2011. 336 с.

16. Коропатов О. М. Поняття та ознаки адміністративно-правового режиму конфіденційної інформації в Україні. *Південноукраїнський правничий часопис*. 2022. № 3. С. 145–150. URL: http://dspace.oduvs.edu.ua/handle/123456789/4047 (дата звернення: 11.04.2024).

17. Кравченко О. М. Конфіденційна інформація та комерційна таємниця в Україні. *Екологічне право*. 2023. № 1. С. 24–29. URL: http://ecolaw.idpnan.kyiv.ua/archive/2023/1-2/1-2_2023.pdf#page=24 (дата звернення: 11.04.2024).

18. Кравченко О. М. Організаційно-правові заходи забезпечення охорони конфіденційної інформації та комерційної таємниці бізнесу в Україні. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Юридичні науки.* Київ, 2023. № 3. С. 48–53. URL:

http://www.juris.vernadskyjournals.in.ua/journals/2023/3_2023/3_2023.pdf#page=54 (дата звернення: 11.04.2024).

19. Кравченко О. М. Охорона конфіденційної інформації та комерційної таємниці в умовах воєнного стану. *Науковий вісник Дніпров. держ. ун-ту внутр. справ.* 2022. № 2. С. 476–480. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/04/S2/s-2-2022-476-480.pdf (дата звернення: 11.04.2024).

20. Кримінальний кодекс України: Закон України від 05.04.2001 р. №2341-III. URL: https://zakon.rada.gov.ua/laws/ show/2341-14#Text (дата звернення: 18.04.2024).

21. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. Дата оновлення: 05.02.2023. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n1498 (дата звернення: 18.04.2024).

22. Ліпкан В. А., Сопілко І. М., Кір'ян В. О. Правові засади розвитку інформаційного суспільства в Україні : монографія. Київ : ФОП О. С. Ліпкан, 2015. 664 с.

23. Логінова Н. І. Правовий захист інформації: навч. посіб. Одеса, 2015. 264 с.

24. Манжай О. В. Правові засади захисту інформації: підручник Харків, 2020. 162 с.

25. Мороз Н. Поняття інформації обмеженого доступу. *Вісник Національного університету «Львівська політехніка». Серія : Юридичні науки*. 2017. № 865. С. 284–289. URL: http://nbuv.gov.ua/UJRN/vnulpurn_2017_865_45 (дата звернення: 15.04.2024)

26. Охорона конфіденційної інформації та комерційної таємниці: як? що? навіщо? URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ohorona-konfidenciynoyi-informaciyi-ta-komerciynoyi-taemnici-yak-shcho-navishcho.html (Дата звернення: 17.05.2024).

27. Правовий захист комерційної таємниці. URL: https://ukrainepravo.com/scientific-thought/pravova-pozytsiya/pravoviy-zakhist-komerts-yno-ta-mnits/ (дата звернення: 17.04.2024).

28. Про банки і банківську діяльність: Закон України від 07.12.2000. URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text (Дата звернення: 17.05.2024).

29. Про державну таємницю: Закон України від 21.01.1994. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (Дата звернення: 17.05.2024).

30. Про доступ до публічної інформації: Закон України від 13.01.2011. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (Дата звернення: 17.05.2024).

31. Про електронні документи та електронний документообіг: Закон України від 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (Дата звернення: 11.03.2024).

32. Про електронний цифровий підпис: Закон України від 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/852-15#Text (Дата звернення: 11.03.2024).

33. Про захист персональних даних: Закон України від 01.06.2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Дата звернення: 17.05.2024).

34. Про інформацію: Закон України від 02.20.1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (Дата звернення: 17.05.2024).

35. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Дата звернення: 17.05.2024).

36. Про телекомунікації: Закон України від 18.11.2003. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text (Дата звернення: 17.05.2024).

37. Сеник С. В. Нормативно-правові засади обігу конфіденційної інформації в Україні. *Соціально-правові студії.* 2021. №3. С. 41–49. URL:

https://dspace.lvduvs.edu.ua/handle/1234567890/3972 (дата звернення: 11.04.2024).

38. Цивільний кодекс України від 16.01.2003 № 435. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 10.04.2024).

39. Цивільний процесуальний кодекс України від 18.03.2004 № 1618. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 10.04.2024).

40. Ярмакі Х. П. Класифікація конфіденційної інформації. *Південноукраїнський правничий часопис*. 2021. № 1. С. 94–98. URL: http://dspace.oduvs.edu.ua/handle/123456789/1768 (дата звернення: 11.04.2024).