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

КУРСОВА РОБОТА

з дисципліни: **«ІНФОРМАЦІЙНЕ ПРАВО»**

за темою: **«ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ»**

Студента (ки): Замлинського Р.О.
курсу:
групи: ІН16-9-22-Б1П (4.0д)
Спеціальність: 081 Право
Керівник: доцент, к.ю.н. Лебедєв О.П.

Оцінка: _____
Національна шкала_____
Кількість балів: _____ ECTS _____

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

м. Чернігів 2026

Зміст

ВСТУП

В умовах стрімкого розвитку інформаційного суспільства інформація набуває стратегічного значення для функціонування держави, суспільства та особистості. Сучасні інформаційні технології забезпечують широкі можливості для обробки, передачі та збереження інформації, однак одночасно створюють нові виклики та загрози, пов’язані з її захистом. У зв’язку з цим питання забезпечення інформаційної безпеки держави набуває особливої актуальності, оскільки вона є важливою складовою національної безпеки та одним із ключових чинників стабільності суспільства.

Інформаційна безпека держави охоплює широкий спектр суспільних відносин, пов’язаних із захистом інформаційного простору, протидією дезінформації, кіберзагрозам, інформаційним війнам, а також забезпеченням прав і свобод людини у сфері інформації. Особливої ваги ця проблема набуває в умовах сучасних геополітичних викликів, зокрема інформаційної агресії, що здійснюється проти України. У таких умовах ефективне функціонування системи інформаційної безпеки є необхідною передумовою збереження державного суверенітету та територіальної цілісності.

Проблематика інформаційної безпеки держави є предметом дослідження багатьох вітчизняних і зарубіжних науковців. Значний внесок у розвиток теоретичних і практичних аспектів забезпечення інформаційної безпеки зробили сучасні дослідники у сфері інформаційного права, національної безпеки та кібербезпеки. Водночас постійний розвиток інформаційних технологій та поява нових загроз зумовлюють необхідність подальшого наукового осмислення цієї проблематики та пошуку ефективних механізмів її вирішення.

Метою курсової роботи є комплексне дослідження інформаційної безпеки держави, визначення її сутності, місця у системі національної безпеки, аналіз сучасних загроз та проблем у цій сфері, а також розроблення пропозицій щодо вдосконалення механізмів її забезпечення.

Для досягнення поставленої мети передбачається вирішення таких завдань: розкрити поняття та сутність інформаційної безпеки держави; визначити її місце у системі національної безпеки; дослідити нормативно-правове забезпечення інформаційної безпеки; проаналізувати сучасні загрози та

виклики у цій сфері; оцінити ефективність державної політики щодо забезпечення інформаційної безпеки; сформулювати пропозиції щодо вдосконалення правового регулювання та практики забезпечення інформаційної безпеки.

Об’єктом дослідження є суспільні відносини, що виникають у сфері забезпечення інформаційної безпеки держави.

Предметом дослідження є теоретичні засади інформаційної безпеки, норми чинного законодавства України, що регулюють цю сферу, а також сучасні наукові підходи до розуміння та забезпечення інформаційної безпеки держави.

Методологічну основу курсової роботи становить сукупність загальнонаукових та спеціально-юридичних методів пізнання. У роботі використано діалектичний метод для дослідження розвитку інформаційної безпеки, системно-структурний метод – для аналізу її місця у системі національної безпеки, логічні методи (аналіз, синтез, індукція, дедукція) – для узагальнення наукових підходів, а також формально-юридичний метод для дослідження нормативно-правового регулювання.

Базу дослідження становлять Конституція України, закони України, укази Президента України, інші нормативно-правові акти, що регулюють сферу інформаційної безпеки, а також наукові праці, статті, монографії та матеріали науково-практичних конференцій.

Курсова робота складається зі вступу, трьох розділів, поділених на підрозділи, висновків та списку використаних джерел. У першому розділі розглядаються теоретичні основи інформаційної безпеки держави. Другий розділ присвячений аналізу сучасного стану та основних загроз інформаційній безпеці України. У третьому розділі досліджуються шляхи вдосконалення системи забезпечення інформаційної безпеки держави.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Поняття та сутність інформаційної безпеки держави

В умовах становлення інформаційного суспільства інформація виступає одним із ключових ресурсів держави поряд із матеріальними, фінансовими та людськими ресурсами. Її значення постійно зростає у зв'язку з розвитком цифрових технологій, глобалізаційними процесами та активним використанням інформаційно-комунікаційних систем у всіх сферах суспільного життя. Саме тому забезпечення інформаційної безпеки держави стає одним із пріоритетних напрямів державної політики та важливою складовою системи національної безпеки.

Поняття інформаційної безпеки є багатогранним і розглядається як у правовому, так і в політичному, соціальному та технічному аспектах. У загальному вигляді інформаційну безпеку держави доцільно визначати як стан захищеності життєво важливих інтересів особи, суспільства і держави від внутрішніх і зовнішніх загроз в інформаційній сфері, що забезпечує стабільний розвиток інформаційного простору, захист інформаційних ресурсів, а також недопущення негативного інформаційного впливу [11, с. 124].

З правової точки зору інформаційна безпека держави є складовою національної безпеки, що охоплює систему правових, організаційних, технічних та інших заходів, спрямованих на захист інформаційних відносин. Вона включає забезпечення цілісності, конфіденційності та доступності інформації, а також захист інформаційних прав і свобод людини, зокрема права на інформацію, свободи слова та захисту персональних даних [10, с. 35].

Сутність інформаційної безпеки держави полягає у забезпеченні такого стану інформаційного середовища, за якого мінімізуються ризики негативного впливу інформації на свідомість громадян, функціонування державних інституцій та суспільні процеси. Це передбачає не лише захист інформаційних систем і ресурсів, але й протидію інформаційним маніпуляціям, пропаганді, дезінформації та іншим формам інформаційного впливу [12, с. 58].

Особливістю інформаційної безпеки є її комплексний характер, оскільки вона охоплює різні сфери суспільного життя. Зокрема, можна виділити такі основні складові інформаційної безпеки держави:

- технічна (кібернетична) безпека, що передбачає захист інформаційно-телекомунікаційних систем від несанкціонованого доступу, кібератак та інших технічних загроз;
- інформаційно-психологічна безпека, спрямована на захист свідомості громадян від маніпулятивного впливу, дезінформації та інформаційних кампаній;
- правова безпека, яка забезпечує належне нормативно-правове регулювання інформаційних відносин;
- організаційна безпека, що включає діяльність державних органів та інституцій у сфері забезпечення інформаційної безпеки [6, с. 45].

Значення інформаційної безпеки держави полягає в тому, що вона безпосередньо впливає на стабільність політичної системи, економічний розвиток, обороноздатність країни та рівень довіри громадян до державних інституцій. У сучасних умовах інформаційна безпека стає інструментом геополітичного впливу, оскільки інформаційні технології активно використовуються для досягнення політичних, економічних і військових цілей.

Особливої актуальності питання інформаційної безпеки набули в умовах гібридних конфліктів, де поряд із традиційними військовими засобами активно застосовуються інформаційні впливи. Такі впливи можуть проявлятися у вигляді поширення фейкової інформації, інформаційних операцій, спрямованих на дестабілізацію суспільства, підрив довіри до державних органів, формування негативного іміджу держави на міжнародній арені [8, с. 114].

Важливою складовою інформаційної безпеки є також кібербезпека, яка охоплює захист інформаційних систем від кіберзагроз. З розвитком цифрових технологій кількість кібератак постійно зростає, що створює значні ризики для функціонування державних органів, критичної інфраструктури та приватного сектору. У зв’язку з цим держава повинна приділяти особливу увагу розвитку системи кіберзахисту, впровадженню сучасних технологій захисту інформації та підготовці кваліфікованих фахівців [9, с. 100].

Суттєвим аспектом інформаційної безпеки є баланс між забезпеченням безпеки та дотриманням прав і свобод людини. Надмірне втручання держави у інформаційну сферу може призвести до обмеження свободи слова та інших демократичних прав. Тому важливо забезпечити гармонійне поєднання заходів безпеки з гарантіями прав людини, що є однією з ознак демократичної правової держави [10, с. 37].

Таким чином, інформаційна безпека держави є складним і багатокомпонентним явищем, яке охоплює різні аспекти суспільного життя та потребує комплексного підходу до її забезпечення. Вона виступає невід'ємною складовою національної безпеки та відіграє ключову роль у забезпеченні стабільності, суверенітету та розвитку держави. Ефективне функціонування системи інформаційної безпеки можливе лише за умови поєднання правових, організаційних та технічних заходів, а також активної участі держави, суспільства та громадян у протидії сучасним інформаційним загрозам.

1.2. Місце інформаційної безпеки в системі національної безпеки держави

Національна безпека держави є складним багатовимірним явищем, що охоплює сукупність суспільних відносин, спрямованих на захист життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз. У сучасних умовах інформаційна складова національної безпеки набуває особливого значення, оскільки інформаційна сфера перетворилася на один із ключових просторів протистояння між державами, а також на важливий інструмент впливу на суспільні процеси.

Інформаційна безпека є невід'ємною складовою національної безпеки держави, оскільки забезпечує захист інформаційного простору, інформаційних ресурсів та інформаційних процесів від загроз, що можуть завдати шкоди державним інтересам. Вона тісно пов'язана з іншими складовими національної безпеки, такими як політична, економічна, воєнна, соціальна та екологічна безпека, і впливає на їх ефективне функціонування [11, с. 126].

Особливість інформаційної безпеки полягає в її універсальному характері. Вона пронизує всі сфери суспільного життя та виступає як

інтегруючий елемент системи національної безпеки. Наприклад, у політичній сфері інформаційна безпека забезпечує стабільність державного управління, захист демократичних інститутів від інформаційного впливу та маніпуляцій. В економічній сфері вона спрямована на захист інформаційних ресурсів підприємств, фінансових систем та комерційної інформації. У воєнній сфері інформаційна безпека є складовою інформаційної боротьби та кібероборони держави [6, с. 48].

Важливим аспектом є те, що інформаційна безпека безпосередньо впливає на реалізацію державної політики у сфері національної безпеки. Вона забезпечує інформаційну підтримку управлінських рішень, формування позитивного іміджу держави на міжнародній арені та протидію інформаційним загрозам, що можуть дестабілізувати суспільство. У цьому контексті інформаційна безпека виступає не лише як захисний механізм, але і як активний інструмент державного впливу [10, с. 36].

Законодавство України визначає інформаційну безпеку як один із пріоритетних напрямів забезпечення національної безпеки. Відповідно до сучасних нормативно-правових актів, держава зобов’язана забезпечувати захист інформаційного простору, протидіяти інформаційним загрозам, розвивати національну інформаційну інфраструктуру та сприяти підвищенню рівня інформаційної культури суспільства. Це свідчить про високий рівень значущості інформаційної безпеки в системі державних пріоритетів.

Суттєвою особливістю інформаційної безпеки як складової національної безпеки є її динамічний характер. На відміну від традиційних сфер безпеки, інформаційна сфера швидко змінюється під впливом технологічного прогресу. З’являються нові форми загроз, зокрема кіберзлочинність, інформаційні війни, використання соціальних мереж для маніпуляції громадською думкою, що вимагає постійного оновлення підходів до забезпечення безпеки [12, с. 60].

Особливу роль інформаційна безпека відіграє в умовах сучасних гібридних загроз. Вона стає одним із ключових інструментів ведення так званих «гібридних війн», де поряд із військовими діями активно використовуються інформаційні операції, спрямовані на підрив державності, послаблення суспільної єдності та дискредитацію органів влади. У таких умовах

інформаційна безпека набуває стратегічного значення та стає одним із головних напрямів державної політики [8, с. 115].

Не менш важливим є взаємозв'язок інформаційної безпеки з кібербезпекою. Кіберпростір стає одним із основних середовищ функціонування держави, тому його захист є невід'ємною частиною забезпечення національної безпеки. Порушення функціонування інформаційних систем може призвести до серйозних наслідків, зокрема порушення роботи органів державної влади, банківської системи, енергетичної інфраструктури та інших критично важливих об'єктів [9, с. 101].

Водночас інформаційна безпека повинна забезпечувати баланс між інтересами держави та правами людини. У демократичному суспільстві важливо не допустити надмірного обмеження свободи слова та доступу до інформації під приводом забезпечення безпеки. Саме тому ефективна система інформаційної безпеки має ґрунтуватися на принципах верховенства права, законності та поваги до прав і свобод людини [10, с. 38].

Таким чином, інформаційна безпека займає ключове місце в системі національної безпеки держави, виступаючи як її важлива складова та інтегруючий елемент. Вона забезпечує захист інформаційного простору, сприяє стабільному розвитку держави та відіграє важливу роль у протидії сучасним загрозам. Ефективне функціонування системи інформаційної безпеки є необхідною умовою забезпечення національної безпеки та сталого розвитку держави в умовах сучасних викликів.

1.3. Нормативно-правове забезпечення інформаційної безпеки держави

Ефективне забезпечення інформаційної безпеки держави неможливе без належного нормативно-правового регулювання, яке визначає основні принципи, напрями, механізми та інструменти захисту інформаційного простору. В Україні сформована певна система нормативно-правових актів, що регулюють відносини у сфері інформаційної безпеки, однак вона продовжує розвиватися відповідно до сучасних викликів і загроз.

Основу нормативно-правового забезпечення інформаційної безпеки становить Конституція України, яка закріплює фундаментальні права і свободи

людини у сфері інформації, зокрема право на свободу думки і слова, на вільне вираження поглядів і переконань, а також право на інформацію. Водночас Конституція встановлює можливість обмеження цих прав в інтересах національної безпеки, що створює правову основу для забезпечення інформаційної безпеки держави [1].

Важливе місце у системі правового регулювання займає законодавство у сфері національної безпеки. Законодавчі акти визначають інформаційну безпеку як складову національної безпеки та встановлюють основні напрями державної політики у цій сфері. Зокрема, законодавство передбачає необхідність захисту інформаційного суверенітету держави, протидії інформаційним загрозам, розвитку інформаційної інфраструктури та забезпечення кібербезпеки [2].

Окрему групу нормативно-правових актів становлять закони, що безпосередньо регулюють інформаційні відносини. Вони визначають правові засади створення, збирання, обробки, зберігання, використання та захисту інформації. Значну увагу в цих актах приділено питанням захисту інформації в інформаційно-телекомунікаційних системах, що є особливо актуальним в умовах цифровізації суспільства та розвитку електронного урядування [10, с. 36].

Важливим елементом нормативного забезпечення є законодавство у сфері кібербезпеки, яке визначає організаційні та правові засади захисту кіберпростору. Воно встановлює повноваження державних органів у сфері кіберзахисту, порядок взаємодії між ними, а також основні напрями державної політики щодо протидії кіберзагрозам. У сучасних умовах кібербезпека виступає невід’ємною складовою інформаційної безпеки, оскільки більшість інформаційних процесів здійснюється саме у цифровому середовищі [9, с. 102].

Особливе значення мають стратегічні документи, що визначають довгострокові напрями розвитку інформаційної безпеки держави. До них належать доктрини, стратегії та концепції, які формують основні підходи до забезпечення інформаційної безпеки, визначають пріоритети державної політики та механізми їх реалізації. Такі документи спрямовані на підвищення ефективності державного управління у сфері інформаційної безпеки та адаптацію до сучасних викликів [6, с. 47].

Система нормативно-правового забезпечення інформаційної безпеки також включає підзаконні нормативні акти, що деталізують положення законів та визначають порядок їх реалізації. Це можуть бути постанови уряду, нормативні акти центральних органів виконавчої влади, інструкції та інші документи, що регулюють окремі аспекти забезпечення інформаційної безпеки. Вони відіграють важливу роль у практичній реалізації державної політики у цій сфері.

Важливим аспектом нормативно-правового забезпечення є також міжнародно-правове співробітництво. Україна бере участь у міжнародних ініціативах у сфері інформаційної та кібербезпеки, що сприяє гармонізації національного законодавства з міжнародними стандартами. Міжнародні договори, рекомендації та стандарти відіграють важливу роль у формуванні сучасної системи інформаційної безпеки та підвищенні її ефективності [12, с. 62].

Разом із тим, незважаючи на наявність розгалуженої системи нормативно-правових актів, існують певні проблеми у правовому регулюванні інформаційної безпеки. Зокрема, спостерігається фрагментарність законодавства, наявність колізій між окремими нормативними актами, а також недостатня узгодженість між різними суб’єктами забезпечення інформаційної безпеки. Крім того, швидкий розвиток інформаційних технологій зумовлює необхідність постійного оновлення законодавства та адаптації його до нових викликів [8, с. 116].

Окремою проблемою є забезпечення ефективного правозастосування. Навіть за наявності належної нормативної бази її ефективність залежить від рівня реалізації норм на практиці. Це потребує належної координації діяльності державних органів, підвищення рівня професійної підготовки фахівців у сфері інформаційної безпеки, а також удосконалення механізмів контролю та відповідальності [11, с. 128].

Таким чином, нормативно-правове забезпечення інформаційної безпеки держави є складною та багаторівневою системою, що включає Конституцію України, закони, підзаконні нормативні акти, стратегічні документи та міжнародні стандарти. Воно відіграє ключову роль у формуванні ефективної системи захисту інформаційного простору та протидії сучасним загрозам.

Водночас подальший розвиток законодавства у цій сфері має бути спрямований на усунення існуючих недоліків, підвищення узгодженості нормативних актів та адаптацію до умов сучасного інформаційного середовища.

РОЗДІЛ 2. СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Основні загрози інформаційній безпеці держави

Сучасний етап розвитку суспільства характеризується стрімкою інформатизацією та цифровізацією практично всіх сфер життя, що, з одного боку, створює нові можливості для розвитку держави, а з іншого — значно підвищує рівень вразливості інформаційного простору до різноманітних загроз. У зв'язку з цим проблема забезпечення інформаційної безпеки держави набуває системного характеру та потребує комплексного підходу до аналізу сучасних ризиків.

Однією з найбільш небезпечних загроз є **інформаційна агресія**, яка в сучасних умовах виступає складовою гібридної війни. Вона реалізується через цілеспрямовані інформаційні кампанії, спрямовані на формування викривленого сприйняття реальності, дискредитацію державних органів, поширення панічних настроїв серед населення та підрив суспільної довіри. Інформаційна агресія може здійснюватися як через традиційні засоби масової інформації, так і через цифрові платформи, соціальні мережі, месенджери, що значно ускладнює її виявлення та протидію [8, с. 114].

Особливу небезпеку становить **дезінформація**, яка є цілеспрямованим поширенням неправдивих або маніпулятивно викривлених відомостей. У сучасних умовах дезінформація набуває масового характеру та може швидко поширюватися завдяки алгоритмам соціальних мереж. Вона здатна впливати на політичні процеси, формувати громадську думку, провокувати соціальні конфлікти та навіть впливати на міжнародні відносини. Застосування новітніх технологій, зокрема штучного інтелекту, значно ускладнює процес розпізнавання дезінформації [12, с. 60].

Не менш важливою загрозою є **кіберзлочинність**, яка охоплює широкий спектр протиправних дій у кіберпросторі. До таких дій належать кібератаки на державні органи, банківські установи, підприємства, а також використання шкідливого програмного забезпечення для викрадення або знищення інформації.

Особливу небезпеку становлять атаки на об’єкти критичної інфраструктури, які можуть призвести до масштабних порушень функціонування держави [9, с. 101].

Серед загроз також слід виділити **витік інформації**, який може мати як технічний, так і організаційний характер. Витік конфіденційної інформації, державної таємниці або персональних даних може спричинити значні негативні наслідки, включаючи порушення прав громадян, економічні втрати та загрозу національній безпеці. Причинами таких витоків можуть бути як недосконаліть систем захисту, так і людський фактор [11, с. 125].

Окремо варто звернути увагу на **загрози інформаційно-психологічного характеру**, які спрямовані на вплив на свідомість громадян. До них належать пропаганда, маніпуляція інформацією, створення інформаційних приводів для формування негативного ставлення до державних інституцій. Такі загрози є особливо небезпечними, оскільки вони впливають не лише на окремих осіб, але й на суспільство в цілому [6, с. 48].

Важливим аспектом є також **технологічні загрози**, пов’язані з розвитком цифрових технологій. Використання штучного інтелекту, автоматизованих систем обробки інформації, а також глобальних інформаційних платформ створює нові можливості для здійснення інформаційного впливу та кіберзлочинності. Водночас ці технології можуть використовуватися як інструменти захисту, що створює необхідність їх ефективного регулювання [12, с. 61].

Таким чином, сучасні загрози інформаційній безпеці держави є комплексними, багаторівневими та динамічними. Вони потребують постійного моніторингу, аналізу та розробки ефективних механізмів протидії.

2.2. Вплив інформаційних та кіберзагроз на державу

Інформаційні та кіберзагрози в умовах сучасного розвитку інформаційного суспільства набувають системного характеру та здійснюють комплексний вплив на функціонування держави. Їх особливість полягає в тому, що вони здатні одночасно впливати на різні сфери суспільного життя, викликаючи як безпосередні, так і відкладені негативні наслідки. На відміну від

традиційних загроз, інформаційні загрози є більш гнучкими, латентними та часто важко ідентифікуються, що значно ускладнює їх нейтралізацію.

Передусім, суттєвий вплив інформаційні загрози здійснюють на політичну систему держави. Інформаційні операції можуть бути спрямовані на дискредитацію органів державної влади, підрив довіри до політичних інститутів, створення образу неефективного або корумпованого управління. Особливо небезпечним є використання інформаційних технологій під час виборчих процесів. Маніпуляції громадською думкою, поширення фейкових новин, створення штучних інформаційних приводів можуть впливати на результати виборів та формувати викривлене політичне середовище [8, с. 115].

Важливим інструментом впливу є так звані інформаційно-психологічні операції, які спрямовані на зміну поведінки та свідомості громадян. Вони можуть включати створення панічних настроїв, провокування соціальних конфліктів, формування негативного ставлення до державної політики. У результаті таких впливів знижується рівень довіри населення до влади, що може призвести до політичної нестабільності та дестабілізації державного управління.

У економічній сфері інформаційні та кіберзагрози мають не менш значний вплив. Кібератаки на банківські установи, фінансові системи та підприємства можуть призводити до втрати значних фінансових ресурсів, порушення функціонування платіжних систем та зниження довіри до економічних інститутів. Особливо небезпечними є атаки, спрямовані на дестабілізацію фінансового сектору, оскільки вони можуть викликати паніку серед населення та спричинити економічну кризу [9, с. 102].

Крім того, витік комерційної інформації або інтелектуальної власності може негативно впливати на конкурентоспроможність підприємств та економіку держави в цілому. Інформаційні атаки можуть також використовуватися для недобросовісної конкуренції, що створює додаткові ризики для розвитку бізнесу.

У соціальній сфері інформаційні загрози можуть мати серйозні наслідки для стабільності суспільства. Поширення дезінформації може призводити до формування хибних уявлень про події, викликати соціальну напругу та конфлікти між різними групами населення. Особливо небезпечними є

інформаційні кампанії, спрямовані на розпалювання ворожнечі, дискримінації або радикалізації суспільства [12, с. 61].

В умовах кризових ситуацій, таких як воєнні конфлікти або надзвичайні події, вплив інформаційних загроз значно посилюється. Населення стає більш вразливим до інформаційного впливу, що створює сприятливі умови для поширення паніки та дестабілізації суспільства. У таких умовах інформаційна безпека набуває особливого значення як інструмент забезпечення соціальної стабільності.

У воєнній сфері інформаційні та кіберзагрози виступають як важливий елемент сучасних гібридних конфліктів. Інформаційні операції можуть використовуватися для деморалізації військових, поширення неправдивих відомостей про бойові дії, а також для підриву обороноздатності держави. Вони можуть супроводжувати традиційні військові дії або навіть виступати як самостійний інструмент впливу [6, с. 49].

Кіберзагрози у воєнній сфері можуть включати атаки на військові інформаційні системи, засоби зв’язку, системи управління військами. Такі атаки можуть призвести до порушення координації дій, втрати контролю над ситуацією та зниження ефективності оборонних операцій.

Особливу небезпеку становить вплив інформаційних загроз на критичну інфраструктуру держави. Об’єкти енергетики, транспорту, зв’язку, охорони здоров’я та інші системи життєзабезпечення є вразливими до кіберзагроз. Порушення їх функціонування може призвести до масштабних наслідків, включаючи економічні втрати, загрозу життю та здоров’ю населення, а також дестабілізацію держави в цілому [11, с. 127].

Крім того, інформаційні загрози можуть впливати на міжнародний імідж держави. Поширення негативної інформації, дезінформаційні кампанії та інформаційні атаки можуть формувати негативне сприйняття держави на міжнародній арені. Це може призводити до зниження рівня довіри з боку міжнародних партнерів, ускладнення дипломатичних відносин та обмеження міжнародного співробітництва.

Слід також зазначити, що інформаційні та кіберзагрози мають кумулятивний ефект, тобто їх вплив може накопичуватися з часом. Навіть

незначні інформаційні впливи, якщо вони здійснюються систематично, можуть призводити до суттєвих змін у суспільній свідомості та поведінці громадян.

Важливою характеристикою сучасних загроз є їх транснаціональний характер. Інформаційні атаки можуть здійснюватися з будь-якої точки світу, що ускладнює їх ідентифікацію та притягнення винних до відповідальності. Це обумовлює необхідність міжнародного співробітництва у сфері інформаційної безпеки.

Таким чином, вплив інформаційних та кіберзагроз на державу є багатовимірним та охоплює всі основні сфери її функціонування. Він проявляється у політичній, економічній, соціальній та воєнній сферах, а також впливає на міжнародний імідж держави. У зв’язку з цим забезпечення інформаційної безпеки повинно розглядатися як комплексне завдання, що потребує системного підходу та координації зусиль держави, суспільства та міжнародної спільноти.

2.3. Аналіз ефективності державної політики у сфері інформаційної безпеки

Державна політика у сфері інформаційної безпеки є одним із ключових напрямів забезпечення національної безпеки України, оскільки саме держава виступає основним суб’єктом формування та реалізації механізмів захисту інформаційного простору. В умовах сучасних викликів, пов’язаних із глобалізацією, цифровізацією та інформаційною агресією, ефективність державної політики у цій сфері набуває особливого значення.

Система державного управління у сфері інформаційної безпеки в Україні має комплексний характер і включає діяльність різних органів державної влади, що реалізують свої повноваження у межах визначених функцій. До них належать органи законодавчої, виконавчої влади, а також спеціалізовані інституції, відповідальні за кібербезпеку, інформаційну політику та захист державних інформаційних ресурсів. Такий багаторівневий підхід дозволяє охопити різні аспекти інформаційної безпеки, однак водночас створює ризики дублювання функцій і недостатньої координації [6, с. 50].

Одним із важливих напрямів державної політики є формування нормативно-правової бази, яка регулює відносини у сфері інформаційної

безпеки. В Україні прийнято низку законодавчих та підзаконних актів, що визначають основні принципи забезпечення інформаційної безпеки, повноваження органів державної влади та механізми захисту інформаційного простору. Проте, незважаючи на наявність значної кількості нормативних актів, законодавство залишається фрагментарним та не завжди узгодженим між собою, що ускладнює його практичне застосування [12, с. 62].

Суттєвою проблемою є також відставання законодавства від сучасних технологічних викликів. Розвиток інформаційних технологій, зокрема штучного інтелекту, великих даних та цифрових платформ, відбувається значно швидше, ніж оновлення нормативно-правової бази. Це створює ситуацію, коли держава не завжди має ефективні правові інструменти для протидії новим загрозам, таким як кібератаки, дезінформація або використання інформаційних технологій у злочинних цілях.

Важливим аспектом ефективності державної політики є рівень координації між державними органами. На практиці часто спостерігається недостатня взаємодія між різними інституціями, що займаються питаннями інформаційної безпеки. Це може призводити до дублювання функцій, неузгодженості дій та зниження ефективності реагування на загрози. Відсутність єдиного координаційного центру або чітко визначеного механізму взаємодії між органами влади ускладнює реалізацію комплексного підходу до забезпечення інформаційної безпеки [11, с. 128].

Не менш важливою проблемою є недостатній рівень фінансування та технічного забезпечення системи інформаційної безпеки. Ефективна протидія сучасним загрозам потребує значних ресурсів, зокрема для розвитку інформаційних систем, впровадження сучасних технологій захисту та підготовки кваліфікованих фахівців. Обмеженість фінансових ресурсів негативно впливає на можливості держави щодо забезпечення належного рівня інформаційної безпеки.

Слід також звернути увагу на кадрову проблему. Забезпечення інформаційної безпеки потребує висококваліфікованих фахівців у сфері інформаційних технологій, кібербезпеки, права та управління. Водночас існує дефіцит таких спеціалістів, що знижує ефективність реалізації державної

політики. Крім того, недостатній рівень підготовки кадрів може призводити до помилок у прийнятті управлінських рішень та реалізації заходів безпеки.

Важливим напрямом державної політики є розвиток системи кібербезпеки. У сучасних умовах кіберпростір є одним із ключових середовищ функціонування держави, тому його захист має стратегічне значення. Україна здійснює заходи щодо створення національної системи кіберзахисту, однак її ефективність залежить від рівня технічного оснащення, координації між суб'єктами та міжнародного співробітництва [9, с. 102].

Позитивною тенденцією є активізація міжнародного співробітництва у сфері інформаційної безпеки. Україна бере участь у міжнародних програмах та ініціативах, спрямованих на підвищення рівня кіберзахисту, обмін досвідом та впровадження міжнародних стандартів. Це сприяє підвищенню ефективності державної політики та адаптації до глобальних викликів.

Разом із тим важливим аспектом є інформаційна культура суспільства. Ефективність державної політики у сфері інформаційної безпеки значною мірою залежить від рівня обізнаності громадян щодо інформаційних загроз. Низький рівень критичного мислення та інформаційної грамотності сприяє поширенню дезінформації та маніпуляцій. Тому держава повинна приділяти значну увагу освітнім програмам та підвищенню інформаційної культури населення [12, с. 63].

Окремої уваги заслуговує проблема балансу між безпекою та правами людини. Забезпечення інформаційної безпеки не повинно призводити до необґрунтованого обмеження свободи слова, доступу до інформації або інших прав громадян. Надмірне втручання держави у інформаційну сферу може негативно впливати на демократичні процеси та викликати недовіру з боку суспільства. Тому державна політика має ґрунтуватися на принципах верховенства права та пропорційності.

Слід також зазначити, що ефективність державної політики значною мірою залежить від оперативності реагування на загрози. У сучасних умовах інформаційні атаки можуть здійснюватися миттєво, що потребує швидкого та ефективного реагування з боку державних органів. Недостатня оперативність може призводити до значних негативних наслідків та втрати контролю над інформаційною ситуацією.

Таким чином, державна політика у сфері інформаційної безпеки в Україні має як позитивні результати, так і низку проблем, що потребують вирішення. До основних недоліків можна віднести фрагментарність законодавства, недостатню координацію між органами влади, обмеженість ресурсів та кадровий дефіцит. Водночас позитивними є тенденції розвитку нормативної бази, активізація міжнародного співробітництва та підвищення уваги держави до проблем інформаційної безпеки.

У цілому можна зробити висновок, що ефективність державної політики у сфері інформаційної безпеки потребує подальшого вдосконалення, зокрема шляхом підвищення рівня координації, удосконалення законодавства, розвитку технічної бази та підготовки кваліфікованих кадрів. Лише за умови комплексного підходу можливе забезпечення належного рівня інформаційної безпеки держави в умовах сучасних викликів.

РОЗДІЛ 3. ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

3.1. Удосконалення нормативно-правового забезпечення інформаційної безпеки

В умовах сучасного розвитку інформаційного суспільства та стрімкого впровадження цифрових технологій нормативно-правове забезпечення інформаційної безпеки держави набуває ключового значення. Саме правове регулювання визначає рамки функціонування інформаційного простору, встановлює механізми протидії загрозам та забезпечує баланс між інтересами держави і правами громадян.

Однією з основних проблем чинного законодавства у сфері інформаційної безпеки є його фрагментарний характер. Наявність великої кількості нормативно-правових актів, які регулюють окремі аспекти інформаційної діяльності, призводить до відсутності єдиного системного підходу, що ускладнює правозастосування та знижує ефективність забезпечення безпеки [12, с. 62].

У зв’язку з цим доцільним є створення кодифікованого акту, який би систематизував законодавство у сфері інформаційної безпеки та визначив єдині підходи до її забезпечення. Такий підхід дозволить усунути колізії між нормативними актами та підвищити ефективність їх застосування [6, с. 47].

Важливим напрямом є адаптація законодавства до сучасних технологічних викликів. Розвиток штучного інтелекту, цифрових платформ та великих даних створює нові ризики, які не завжди враховані у чинному законодавстві. Це зумовлює необхідність розроблення нових правових механізмів регулювання таких технологій.

Необхідним є також удосконалення правового регулювання кібербезпеки, зокрема шляхом визначення чітких повноважень суб’єктів забезпечення кібербезпеки, порядку їх взаємодії та механізмів реагування на кіберінциденти.

Окремої уваги потребує правове регулювання протидії дезінформації. У сучасних умовах дезінформація є одним із ключових інструментів інформаційного впливу, що може мати серйозні наслідки для держави. Водночас

необхідно забезпечити баланс між протидією дезінформації та дотриманням свободи слова [8, с. 116].

Важливим аспектом є гармонізація національного законодавства з міжнародними стандартами, що сприятиме підвищенню рівня інформаційної безпеки та розвитку міжнародного співробітництва.

Таким чином, удосконалення нормативно-правового забезпечення інформаційної безпеки має здійснюватися комплексно, з урахуванням сучасних викликів та міжнародного досвіду.

3.2. Організаційні та інституційні заходи забезпечення інформаційної безпеки

Організаційні та інституційні механізми відіграють ключову роль у забезпеченні ефективного функціонування системи інформаційної безпеки держави. Від рівня координації між суб'єктами забезпечення інформаційної безпеки залежить ефективність протидії сучасним загрозам.

Однією з основних проблем є недостатня координація між державними органами. Наявність значної кількості суб'єктів у цій сфері призводить до розпорошення повноважень, дублювання функцій та зниження ефективності управління.

У зв'язку з цим доцільним є створення єдиного координаційного центру, який би забезпечував узгодженість дій усіх суб'єктів інформаційної безпеки та підвищував ефективність управління [6, с. 50].

Важливим напрямом є впровадження сучасних систем управління інформаційною безпекою, що базуються на ризик-орієнтованому підході. Це дозволить більш ефективно визначати пріоритети у забезпеченні безпеки та раціонально використовувати ресурси.

Особливу увагу слід приділити розвитку технічної інфраструктури, зокрема впровадженню сучасних засобів кіберзахисту, систем моніторингу та реагування на кіберзагрози.

Важливим є також підвищення рівня професійної підготовки кадрів, що є необхідною умовою ефективного функціонування системи інформаційної безпеки.Крім того, доцільним є розвиток державно-приватного партнерства, яке

дозволить залучити додаткові ресурси та сучасні технології для забезпечення інформаційної безпеки [6, с. 49].

Таким чином, організаційні заходи мають бути спрямовані на підвищення ефективності управління, координації та ресурсного забезпечення системи інформаційної безпеки.

3.3. Перспективи розвитку системи інформаційної безпеки держави

Сучасний етап розвитку інформаційного суспільства характеризується не лише зростанням ролі інформації як стратегічного ресурсу, але й суттєвим ускладненням характеру загроз у цій сфері. У зв'язку з цим розвиток системи інформаційної безпеки держави повинен здійснюватися на основі довгострокового стратегічного підходу, що передбачає не лише реагування на існуючі виклики, але й їх прогнозування та превенцію.

Одним із ключових стратегічних напрямів є перехід від реактивної до проактивної моделі забезпечення інформаційної безпеки. Традиційно державна політика у цій сфері орієнтована на реагування на вже існуючі загрози, що суттєво знижує її ефективність в умовах динамічного розвитку інформаційних технологій. Натомість сучасні умови вимагають формування системи раннього виявлення загроз, прогнозування їх розвитку та запобігання негативним наслідкам ще на стадії їх виникнення [12, с. 62].

Важливим напрямом є інституціоналізація кіберстійкості як базового принципу функціонування держави. Йдеться не лише про захист інформаційних систем, а про забезпечення їх здатності функціонувати в умовах постійного впливу кіберзагроз. Це передбачає створення резервних систем, децентралізацію інформаційної інфраструктури, впровадження механізмів безперервності діяльності та швидкого відновлення після інцидентів [9, с. 101].

Суттєвим стратегічним вектором є інтеграція інформаційної безпеки у всі сфери державної політики. Інформаційна безпека не може розглядатися як ізольована галузь, оскільки вона безпосередньо впливає на політичну стабільність, економічний розвиток, обороноздатність та соціальну згуртованість. У зв'язку з цим необхідним є впровадження принципу "security by

design”, тобто врахування вимог інформаційної безпеки на всіх етапах розроблення та реалізації державних рішень [6, с. 50].

Окремої уваги потребує технологічний розвиток системи інформаційної безпеки. Використання штучного інтелекту, машинного навчання та систем обробки великих даних дозволяє значно підвищити ефективність виявлення аномалій, прогнозування загроз та автоматизації процесів реагування. Водночас впровадження таких технологій потребує належного правового регулювання та контролю, оскільки вони можуть створювати нові ризики, пов’язані з порушенням прав людини та зловживанням інформацією [12, с. 61].

Важливим стратегічним напрямом є розвиток національної інформаційної інфраструктури та цифрового суверенітету. Залежність від іноземних технологій та інформаційних платформ створює додаткові ризики для інформаційної безпеки держави. У зв’язку з цим необхідно забезпечити розвиток власних технологічних рішень, підтримку національних ІТ-компаній та створення захищених державних інформаційних ресурсів [11, с. 127].

Не менш важливим є посилення міжнародної кооперації у сфері інформаційної безпеки. З огляду на транснаціональний характер інформаційних загроз, ефективна протидія їм можлива лише за умов активної взаємодії держав. Це включає обмін інформацією про кіберінциденти, спільні заходи реагування, гармонізацію законодавства та участь у міжнародних ініціативах [11, с. 128].

Суттєвим елементом розвитку системи інформаційної безпеки є формування стійкості суспільства до інформаційних впливів. Йдеться не лише про технічні засоби захисту, але й про підвищення рівня інформаційної грамотності населення, розвиток критичного мислення та здатності до аналізу інформації. У сучасних умовах саме людський фактор є одним із найбільш вразливих елементів системи інформаційної безпеки [12, с. 63].

Окремого значення набуває забезпечення балансу між інформаційною безпекою та правами людини. У процесі посилення заходів безпеки існує ризик надмірного втручання держави у інформаційну сферу, що може призвести до обмеження свободи слова та інших демократичних прав. Тому державна політика повинна базуватися на принципах пропорційності, законності та верховенства права [10, с. 37].

Крім того, перспективним є впровадження ризик-орієнтованого підходу до управління інформаційною безпекою, який дозволяє ефективно розподіляти ресурси та концентрувати зусилля на найбільш критичних напрямках. Такий підхід передбачає постійний аналіз загроз, оцінку їх впливу та адаптацію заходів безпеки до змін у середовищі [6, с. 49].

Таким чином, перспективи розвитку системи інформаційної безпеки держави пов’язані з переходом до проактивної моделі управління, впровадженням інноваційних технологій, зміцненням міжнародного співробітництва та підвищенням стійкості суспільства до інформаційних впливів. Лише за умови комплексного підходу, що поєднує правові, організаційні та технологічні інструменти, можливо забезпечити ефективний захист інформаційного простору держави в умовах сучасних викликів.

ВИСНОВКИ

У результаті проведеного дослідження встановлено, що інформаційна безпека держави є однією з ключових складових національної безпеки, яка в сучасних умовах набуває особливого значення. З розвитком інформаційного суспільства та цифрових технологій інформація перетворюється на стратегічний ресурс, а контроль над інформаційним простором — на важливий фактор забезпечення державного суверенітету та стабільності.

У ході дослідження було з'ясовано сутність інформаційної безпеки держави як стану захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері. Встановлено, що інформаційна безпека має комплексний характер та охоплює правові, організаційні, технічні та соціально-психологічні аспекти. Її значення полягає у забезпеченні стабільності державного управління, захисті інформаційних ресурсів, протидії інформаційним впливам та збереженні прав і свобод громадян.

Дослідження показало, що інформаційна безпека займає важливе місце в системі національної безпеки держави, виступаючи інтегруючим елементом, який впливає на функціонування політичної, економічної, соціальної та воєнної сфер. Встановлено, що в умовах сучасних гібридних загроз інформаційна безпека набуває стратегічного значення та стає одним із ключових напрямів державної політики.

Аналіз нормативно-правового забезпечення інформаційної безпеки в Україні свідчить про наявність сформованої системи правового регулювання, яка включає Конституцію України, закони, підзаконні нормативні акти та стратегічні документи. Водночас виявлено низку проблем, зокрема фрагментарність законодавства, наявність колізій та відставання правового регулювання від сучасних технологічних викликів.

У процесі дослідження встановлено, що сучасні загрози інформаційній безпеці мають комплексний характер та охоплюють як технічні, так і соціально-політичні аспекти. До основних загроз віднесено інформаційну агресію, дезінформацію, кіберзлочинність, витік інформації та вплив на критичну інфраструктуру. Визначено, що ці загрози мають системний характер та здатні впливати на всі сфери функціонування держави.

Оцінка впливу інформаційних та кіберзагроз показала, що вони можуть призводити до дестабілізації політичної системи, порушення економічної діяльності, зростання соціальної напруги та зниження обороноздатності держави. Особливо небезпечним є їх вплив на критичну інфраструктуру та міжнародний імідж держави.

Аналіз ефективності державної політики у сфері інформаційної безпеки дозволив виявити як позитивні тенденції, так і низку проблем. До позитивних аспектів віднесено розвиток нормативно-правової бази, активізацію міжнародного співробітництва та підвищення уваги держави до питань інформаційної безпеки. Водночас визначено проблеми, пов’язані з недостатньою координацією між державними органами, обмеженістю ресурсів, кадровим дефіцитом та необхідністю вдосконалення законодавства.

У роботі обґрунтовано основні напрями вдосконалення системи інформаційної безпеки держави. Зокрема, запропоновано удосконалення нормативно-правового регулювання шляхом його систематизації та адаптації до сучасних викликів, підвищення рівня координації між суб’єктами забезпечення безпеки, розвиток системи кіберзахисту та впровадження сучасних технологій.

Окрему увагу приділено перспективам розвитку системи інформаційної безпеки, серед яких визначено перехід до проактивної моделі управління, забезпечення кіберстійкості держави, розвиток міжнародного співробітництва, а також підвищення рівня інформаційної культури суспільства. Встановлено, що ефективність системи інформаційної безпеки значною мірою залежить від здатності держави адаптуватися до швидких змін у інформаційному середовищі.

Таким чином, у ході дослідження досягнуто поставленої мети та виконано визначені завдання. Отримані результати свідчать про необхідність подальшого вдосконалення системи інформаційної безпеки держави на основі комплексного підходу, що поєднує правові, організаційні та технологічні заходи. Це є необхідною умовою забезпечення національної безпеки та сталого розвитку держави в умовах сучасних викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

А. Нормативно-правові акти

1. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР.
2. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII.
3. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII.
4. Стратегія інформаційної безпеки України : Указ Президента України від 28 грудня 2021 р. № 685/2021.
5. Доктрина інформаційної безпеки України : Указ Президента України від 25 лютого 2017 р. № 47/2017.

Б. Спеціальна література

6. Недохлєбов І. І. Інформаційна безпека України в умовах сучасних загроз: організаційно-правові аспекти : дис. … канд. юрид. наук. Запоріжжя, 2024. 220 с.
7. Босак І. М. Інформаційна безпека України: загрози та методи протидії // Київський економічний науковий журнал. 2025. № 2. С. 45–52.
8. Братах Л. Інформаційна безпека України в умовах дезінформаційного впливу // Політологічний вісник. 2025. № 91. С. 112–118.
9. Селіхов Д. А. Кібербезпека як складова інформаційної безпеки України // Науковий вісник Ужгородського національного університету. Серія: Право. 2026. № 75. С. 98–103.
10. Сопілко І. М. Інформаційна безпека України: поняття та правове забезпечення // Юридичний науковий електронний журнал. 2023. № 5. С. 34–38.
11. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України // Вісник Львівського державного університету внутрішніх справ. 2020. № 2. С. 123–130.
12. Аналіз факторів та сучасних загроз інформаційній безпеці держави у контексті забезпечення національної безпеки України // Наукові праці. 2022. № 4. С. 56–63.

13. Інформаційна безпека суспільства в умовах воєнного стану : матеріали наук.-практ. конф. Київ, 2025. 210 с.

14. Mazurczyk W., Lee D., Vlachos A. Disinformation 2.0 in the Age of AI: A Cybersecurity Perspective // Association for Computing Machinery. 2023. Vol. 1, No. 1. 5 p.