Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий інститут міжнародних відносин
та національної безпеки
Кафедра національної безпеки та політології

Кваліфікаційна робота

на здобуття освітнього ступеня магістра на тему:

«Правове забезпечення інформаційної безпеки України»

Виконав студент ІІ курсу, групи МНб-21,

спеціальності 256 Національна безпека (за окремими

сферами забезпечення і видами діяльності)

Адамський Леонід Володимирович

Керівник – викладач Хомич Тетяна Миколаївна

Рецензент – кандидат юридичних наук, доцент

Стрельбіцька Леся Ярославівна

Острог, 2024

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасному світі, на фоні стрімкого розвитку інформаційних технологій та поширення Інтернету, питання інформаційної безпеки стає однією з найбільш актуальних та нагальних проблем. Україна, як і багато інших країн, постійно стикається зі зростаючими загрозами в цій сфері. З урахуванням війни з Російською Федерацією та постійних кібератак, інформаційна безпека стає ключовим аспектом національної безпеки України.

Перш за все, необхідно визначити, що розуміється під поняттям «правове забезпечення інформаційної безпеки». Це означає наявність ефективного законодавства, спрямованого на захист інформації від небажаних втручань, кібератак, кібер-шпигунства та інших загроз. Таке законодавство має створювати правові умови для запобігання, виявлення та реагування на інформаційні загрози, а також для відновлення національної кіберстійкості.

Сьогодні, коли кіберзлочинці використовують найновітніші технології та вразливості в інформаційних системах для своїх цілей, необхідність ефективного правового регулювання стає безперечною. Україна, була свідком численних кібератак, які спрямовані на державні інституції, критичну інфраструктуру, а також на звичайних громадян. Забезпечення відповідного рівня захисту інформації від таких загроз вимагає наявності не лише технічних заходів, але і сильної правової бази, що забезпечує покарання за кіберзлочини та сприяє превентивним заходам.

Крім того, з урахуванням активного розвитку кіберпростору та зростання кількості кіберзагроз, постійне вдосконалення законодавства є необхідним. Злочинці постійно адаптуються до нових умов, використовуючи нові технології та методи атак.

Тому, правові норми повинні бути гнучкими та здатними швидко реагувати на зміни в кіберзлочинній діяльності. Це завдання, яке вимагає комплексного підходу та спільних зусиль державних і недержавних структур, а

також міжнародного співробітництва. Без ефективного правового захисту інформації неможливо забезпечити стабільність та безпеку в країні в умовах сучасних викликів і загроз.

Метою дослідження є ретельний аналіз існуючого законодавства та правових механізмів, спрямованих на захист інформації від кіберзагроз. Дослідження має на меті виявлення прогалин, недоліків та потреб у вдосконаленні правового поля у цій сфері. Крім того, воно спрямоване на розробку рекомендацій щодо вдосконалення законодавства, зокрема врахування сучасних тенденцій у розвитку кіберзлочинності та міжнародного досвіду. Основною метою є забезпечення належного рівня захисту інформації від кіберзагроз і збереження національної кіберстійкості.

Відповідно до поставленої мети, були сформовані наступні завдання:

1. Висвітлити суть та тлумачення поняття інформаційна безпека України
2. Охарактеризувати чинне законодавство у регулюванні забезпечення інформаційної безпеки України.
3. Розкрити основні напрямки правового регулювання в області забезпечення інформаційної безпеки, системи органів влади та управління.
4. Окреслити системи міжнародної інформаційної безпеки та досвід правового регулювання
5. Визначити основні аспекти нормативного забезпечення інформаційної безпеки України.
6. Оцінка системи інформаційної безпеки України в контексті Євроінтеграції.

Предметом роботи є сутність та особливість забезпечення інформаційної безпеки України, а **об'єктом -** правове забезпечення інформаційної безпеки України.

Аналіз джерел та літератури. За останній час в Україні спостерігаються значні зміни в державній, правовій та інформаційній сферах, такі як адміністративна та судова реформи, реформа правоохоронних органів та системи

національної безпеки. Ці процеси надають особливої актуальності державно-правовому забезпеченню інформаційної безпеки.

Наукове вивчення інформаційної безпеки та системи її забезпечення стає все більш активним не лише в юридичних науках, а й в інших галузях, таких як соціальні та технічні науки.

У теорії держави і права вчені, такі як В. М. Лопатін, Ю. Є. Максименко, Н. В. Римарьова, А. О. Стрельцов, розглядають правові аспекти забезпечення інформаційної безпеки в контексті взаємозв'язків з іншими державними та правовими явищами. У галузевих і прикладних правових науках акцентується увага на адміністративно-правовому, кримінально-правовому, інформаційному праві, а також криміналістиці та цивільному праві, зокрема щодо аспектів інформаційної безпеки. Соціально-гуманітарні науки вивчають інформаційну безпеку з філософсько-соціологічних, політологічних та психологічних позицій.

Загальна складність та динамічність інформаційної безпеки сприяють міждисциплінарному підходу до її вивчення. Це передбачає об'єктивність та обґрунтованість досліджень, системність взаємозв'язків між ними та інтеграцію методологічних підходів різних галузей науки. У сучасних умовах виникають нові виклики для інформаційної безпеки, такі як захист інформаційного суверенітету, боротьба з кіберзлочинністю та кібертероризмом. Тому актуальність державно-правового забезпечення інформаційної безпеки стає більш очевидною і вимагає додаткових наукових досліджень і розробок.

В.А. Ліпкан, Л.С. Харченко та О.В. Логінов описують інформаційну безпеку як процес керування загрозами та небезпеками для державних та недержавних інституцій, окремих громадян, що сприяє забезпеченню інформаційного суверенітету України.

О.А. Баранов розглядає інформаційну безпеку як стан захищеності національних інтересів в інформаційному середовищі, де запобігається заподіяння шкоди державі, суспільству чи особам через незаконне поширення, недостовірність або несвоєчасність інформації.

Л.М. Наливайко також підтримує необхідність забезпечення інформаційної безпеки для національної безпеки України та вказує на загрози інформаційній сфері, що можуть впливати на свідомість та поведінку людей.

О.Д. Довгань і Т.Ю. Ткачук зазначають, що у зв'язку з гібридною агресією Росії особливо актуальною стає протидія поширенню шкідливої інформації та розвиток відповідного законодавства, включаючи питання інформаційно-психологічної безпеки.

Д.О. Хом’яков підкреслює важливість наявності відповідної нормативно-правової бази для створення ефективної системи забезпечення інформаційної безпеки.

Методи дослідження. В процесі виконання магістерської роботи було використано широкий комплекс методів та засобів дослідження, зокрема: метод аналізу нормативно-правових актів, який дозволяє детально вивчити чинне законодавство у сфері інформаційної безпеки, включаючи закони, підзаконні акти, міжнародні договори та стандарти. Це допомагає зрозуміти, як формуються правові основи захисту інформації в Україні. Не менш важливим є порівняльно-правовий метод, за допомогою якого є можливість порівняти правове регулювання інформаційної безпеки в Україні з іншими країнами. Також був застосований історичний метод, який дозволив простежити розвиток правового регулювання інформаційної безпеки в Україні від моменту здобуття незалежності до сьогодення. Це допомогло зрозуміти еволюцію законодавчих ініціатив і адаптацію правової системи до нових викликів.

Структура роботи. Робота складається зі змісту, вступу, чотирьох розділів та семи підрозділів. Список джерел та літератури налічує 63 позиції розташованих на семи сторінках. Загальна кількість сторінок роботи складає 71 аркуш.

РОЗДІЛ І. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Поняття та сутність інформаційної безпеки

Зростання впливу інформаційних ресурсів у сучасному суспільстві, викликане розширенням медіа-сфери, впровадженням новітніх технологій та покращенням інформаційної інфраструктури, підкреслює необхідність звернення уваги до проблеми інформаційної безпеки.

Інформація стає ключовим ресурсом для розвитку суспільства, що не лише не вичерпується, але й постійно зростає, сприяючи підвищенню якості життя, економічному і політичному зростанню країни. Інтенсивний обмін інформацією також відіграє важливу роль у забезпеченні цілісності міжнародного співтовариства.

Однак ця зростаюча залежність від інформації робить суспільство більш вразливим до інформаційної агресії та тероризму, що вимагає належного рівня захисту як на національному, так і на організаційному рівні.

Поняття інформаційної безпеки визначається як захищеність національних інтересів України у цифровому просторі, що враховує рівновагу між потребами особистості, суспільства та держави і відповідає на внутрішні та зовнішні загрози. З іншого боку, воно описує стан інформаційних систем, які забезпечують обіг, функціонування та використання інформації, враховуючи потреби фізичних та юридичних осіб.

Яке ж визначення «інформаційної безпеки» надають науковці?

За визначенням дослідника Р. Калюжного, інформаційна безпека становить сукупність суспільних інформаційних правовідносин, які спрямовані на створення, підтримку, охорону та захист сприятливих умов для життя людини, суспільства і держави. Ці правовідносини пов’язані зі створенням, зберіганням, поширенням і використанням інформації[1].

[1] Калюжний Р. Питання концепції реформування інформаційного законодавства України // Правове, нормативне та метрологічне забезпечення системи інформації в Україні: тематичний збірник праць учасників Другої науково-технічної конференції. Київ, 2000. С. 20.

К. Бєляков також підкреслює, що поняття інформаційної безпеки не обмежується лише технологічними аспектами, але також охоплює правові аспекти захисту інформаційної сфери суспільства, сприяючи її розвитку на користь громадян, організацій і держави в цілому[2]. Водночас Б. Кормич говорить про інформаційну безпеку як про захищеність установлених законом правил, які регулюють інформаційні процеси в державі, тим самим забезпечуючи гарантовані умови існування і розвитку людини, суспільства і держави, як це передбачено Конституцією[3].

У зарубіжних наукових джерелах система інформаційної безпеки зазвичай визначається як система захисту інформації, що містить елементи цілісності, доступності та конфіденційності. У той час, вітчизняні дослідники акцентують увагу на іншій складовій інформаційної безпеки, такі як інформаційно-психологічна та державно-ідеологічна. Більш того, система інформаційної безпеки може включати інші аспекти, такі як соціальний, нормативно-правовий, економічний, фінансовий, військовий, екологічний, програмно-технічний тощо.

Традиційні визначення інформаційної безпеки в цілому відповідають законодавчому визначенню, яке міститься у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». Згідно з цим законом, інформаційна безпека означає захищеність життєво важливих інтересів людини, суспільства і держави, що включає запобігання завданню шкоди через неповноту, невчасність та невірогідність інформації, негативний інформаційний вплив, негативні наслідки застосування інформаційних технологій, а також несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації[4].

---

[2] Бєляков К.І. Деякі питання щодо формування реформи інформаційного законодавства України // Систематизація законодавства в Україні: проблеми теорії і практики: матеріали міжнародної науково-практичної конференції. Київ: Інститут законодавства Верховної Ради України, 1999. С. 254.

[3] Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України Політичний менеджмент. 2008. № 4. С. 135-136.

[4] Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V // Відомості Верховної Ради України.

Поняття «інформаційна безпека» включає інші терміни, такі як «безпека інформаційних технологій», «кібербезпека», «ІТ-безпека» та інші, які становлять складові цієї концепції[5]. Стаття 17 Конституції України відносить інформаційну безпеку до найважливіших функцій держави та обов'язку усього українського народу, нарівні з захистом суверенітету та територіальної цілісності України[6].

Таким чином, інформаційна безпека стає ключовою складовою національної безпеки. Інформаційна сфера відтінена знаннями про інші сфери життєдіяльності суспільства, існуючи як самостійно, так і у взаємозв'язку з іншими сферами. Це підкреслює важливість інформаційної сфери та загрози, що на неї спрямовані. Забезпечення інформаційної безпеки є запорукою для забезпечення інших аспектів національної безпеки, оскільки всі взаємовідносини між суб'єктами суспільства ґрунтуються на споживанні та обміні інформацією.

Доктрина інформаційної безпеки України, яка була затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України» від 29 грудня 2016 року, відводить важливі функції забезпечення інформаційної безпеки таким органам, як Рада національної безпеки і оборони України, Кабінет Міністрів України, Міністерство інформаційної політики України, Міністерство закордонних справ України, Міністерство оборони України, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Служба безпеки України, Розвідувальні органи України, та Державна служба спеціального зв’язку й захисту інформації України[7].

На відміну від системи інформаційної безпеки, система забезпечення інформаційної безпеки має свої власні закономірності, які можна

[5] Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження // Юридичний вісник. 2021. 1 (58). С. 96.
[6] Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР: із змінами та доповненнями від 01.01.2020 р. № 27-IX // Відомості Верховної Ради України.
[7] Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Презедента України від 13.02.2017 №47 // Відомості Верховної Ради України.

використовувати як аналогічні тим, що спостерігаються у системі національної безпеки та її забезпечення[8].

Структура «забезпечення інформаційної безпеки» включає в себе кілька ключових аспектів: предмет та об'єкт безпеки, загрози об'єкту безпеки, діяльність щодо захисту об'єкта безпеки від загроз, а також засоби і суб'єкти, що забезпечують безпеку[9].

Основними об'єктами інформаційної безпеки є інформація, пов'язана з національними інтересами (включаючи будь-які дані, що можуть зберігатися на різних носіях або в електронному вигляді), інформаційна інфраструктура та правовий статус суб'єктів інформаційної сфери.

У широкому розумінні об'єктами правового забезпечення інформаційної безпеки є особа (з її правами і свободами на збирання, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних; захищеність від негативного інформаційно-психологічного впливу), суспільство (його матеріальні і духовні цінності), конституційний лад, суверенітет і територіальна цілісність держави.

Суб'єктами забезпечення інформаційної безпеки можуть бути органи, організації та окремі особи, які мають відповідні повноваження відповідно до закону. Загалом, діяльність держави у цій сфері, яка втілюється через правові норми, має на меті забезпечення інформаційної безпеки як один з основних пріоритетів[10].

О. Довгань пропонує комплексну модель системи забезпечення інформаційної безпеки, яка охоплює широкий спектр об'єктів та суб'єктів інформаційної безпеки. Згідно з його концепцією, об'єктами інформаційної

[8] Сливка М.М., Лук'янова Г.Ю. Правове забезпечення інформаційної безпеки: досвід країн Європейського Союзу // Юридичний науковий електронний журнал. 2021. № 11. С. 515.
[9] Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження // Юридичний вісник. 2021. 1 (58). С. 97.
[10] Довгань О.Д., Ткачук Т.Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс // Інформація і право. 2018. № 2 (25). С. 74.

безпеки є такі важливі аспекти як конституційні права та свободи людини і громадянина, здоров'я населення (фізичне та психологічне), захист від деструктивного та маніпулятивного інформаційного впливу, інформаційне забезпечення та гарантії прав на інформацію та розвиток усіх регіонів України, а також національний інформаційний суверенітет та безпека інформаційної інфраструктури[11].

У цій системі суб'єктами забезпечення інформаційної безпеки є різноманітні установи та органи влади, включаючи Президента, Верховну Раду та Кабінет Міністрів України, Раду національної безпеки і оборони, Національний банк, а також міністерства, комітети та служби, що відповідають за різні аспекти інформаційної безпеки. Серед них Міністерство інформаційної політики, Державний комітет телебачення і радіомовлення, Національна рада з телебачення і радіомовлення, Служба спеціального зв'язку і захисту інформації, а також правоохоронні та військові структури[12].

Пилипчук В. додає до цього списку додаткові суб'єкти, такі як Міністерство юстиції, Національна комісія з питань зв'язку та інформатизації, а також різні державні та недержавні органи, підприємства та організації. Важливими викликами в інформаційній сфері, які він визначає, є проблеми ефективності державної інформаційної політики та кібербезпеки, а також захист прав і свобод людини та громадянина. Такий підхід дозволяє отримати комплексне уявлення про систему забезпечення інформаційної безпеки, враховуючи різноманітні аспекти та учасників цього процесу[13].

Суть інформаційної безпеки можна узагальнити як комплекс заходів, спрямованих на забезпечення права на інформацію та свободи інформаційної діяльності, а також на захист інформації та прав власності на неї, відповідно до загальноприйнятих норм і стандартів. Це означає, що метою інформаційної

[11] Довгань О. Д. Сучасні інформаційні структури як компоненти інформаційної безпеки // Інформація і право. 2015. № 2(14). С. 119.
[12] Там само. С. 119-120.
[13] Пилипчук В.Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми // Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти: матеріали наук-практ. конф. (6 жовтня 2016 р., м. Київ). Київ: НТУУ «КПІ ім. Ігоря Сікорського», Вид-во «Політехніка», 2016. С. 25-26.

безпеки є не лише захист від зовнішніх загроз, а й забезпечення цілісності та конфіденційності інформації, щоб вона не потрапляла в неповноважні руки або не використовувалася з порушенням закону.

Згідно з твердженням Б. Кормича, інформаційна безпека складається з суб'єктно-об'єктного складу, який включає інформаційну безпеку особи, суспільства та держави. Це означає, що держава, людина і суспільство одночасно виступають як суб'єкти та об'єкти інформаційної безпеки, захищаючи важливу для них інформацію та інформаційні процеси[14].

О. Довгань розглядає інформаційні структури як компоненти системи інформаційної безпеки, а також вважає інформаційний суверенітет її об'єктом. Також поняття системи інформаційної безпеки охоплює інші аспекти, такі як інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології[15].

О. Тихомиров вважає, що інформаційна безпека полягає в стані оптимального функціонування і розвитку інформаційної системи в цілому та її елементів окремо. Він пропонує широкий спектр критеріїв для побудови системи інформаційної безпеки, які охоплюють різні сфери суспільного життя, об'єкти національної безпеки, сучасні аспекти розуміння інформаційної безпеки, форми державного забезпечення, напрями пізнавального процесу в галузі забезпечення, засоби забезпечення та інші[16].

Методологія формування системи забезпечення інформаційної безпеки та практичні заходи для вирішення цих завдань демонструють, що успішність будь-якої частини цієї системи прямо залежить від ефективності всієї структури, в яку вона вплетена. Це означає, що кожен елемент цієї системи повинен працювати гармонійно, спільно спрямовуючи зусилля на досягнення загальної мети - забезпечення інформаційної безпеки в усіх її аспектах.

---

[14] Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2003. С. 29.

[15] Довгань О. Д. Сучасні інформаційні структури як компоненти інформаційної безпеки // Інформація і право. 2015. № 2(14). С. 115-116.

[16] Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія. Київ: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. С. 55-56.

Залежність української інформаційної інфраструктури від зарубіжних технологій стала фактом через низьку конкурентоспроможність національної мікроелектроніки, телекомунікаційного обладнання, обчислювальної техніки та програмного забезпечення. Більшість інформаційних та телекомунікаційних систем в Україні створено за участю зарубіжних технологій [17].

Проте важливо враховувати, що розширення використання інформаційних технологій призводить до зростання загроз національній безпеці. Зростання соціальної небезпеки зумовлене збільшенням протиправної діяльності в інформаційній сфері, що вимагає посилення захисту критично важливих об'єктів інформаційної інфраструктури та боротьби з комп'ютерною злочинністю, включаючи кібертероризм[18].

Інформаційна безпека є не просто станом чи умовою життєдіяльності суспільства, але й сприятливим середовищем для розвитку особистості, суспільства та держави. Крім того, вона включає в себе проблеми культурної експансії, збереження мовної та національної ідентичності, а також протидію недоброякісній чи хибній інформації. Розуміння цієї концепції дозволяє визначити, кому, що, і які загрози, а також розробити механізми протидії цим загрозам.

В. Пилипчук та О. Дзьобань перелічують основні види загроз інформаційній безпеці, до яких відносяться: витіснення вітчизняних інформаційних агентств та посилення залежності від закордонних структур, маніпулювання інформацією, вплив іноземних політичних та економічних структур на зовнішню політику, дезінформація про зовнішню політику, порушення прав громадян та юридичних осіб в інформаційній сфері, та спроби несанкціонованого доступу до інформації[19].

---

[17] Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в України // Право і суспільство. 2012. № 3. С. 135.

[18] Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні // Підприємництво, господарство і право. 2019. № 9. С. 102-103.

[19] Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці в інформаційній сфері // Вісник Національної академії правових наук України. 2014. № 3 (78). С. 43-52.

Забезпечення безпеки передбачає не лише збереження поточного стану, але й створення можливостей для переходу на новий, більш високий рівень розвитку. Тому безпеку слід розглядати не як статичний стан об'єкта, а як його здатність до росту, розширення та прогресивного розвитку навіть в умовах внутрішніх конфліктів, невизначеності та ризику.

Важливо усвідомити, що інформаційна безпека не зводиться до «захисту інтересів», оскільки інтереси визначаються як потреби, що необхідні для нормального функціонування суспільства. Тому мета полягає не в захисті цих інтересів, а в їх реалізації.

Отже, інформаційна безпека включає у себе інтереси особи, суспільства та держави, а також забезпечує якість систем, необхідних для задоволення потреб різних суб'єктів. Для забезпечення цієї безпеки держава визначає відповідні органи та механізми, що регулюють і контролюють інформаційні процеси. Важливим аспектом є залежність української інформаційної інфраструктури від зарубіжних технологій, що вимагає уваги до заходів захисту національних інтересів в цій сфері. Загалом, розуміння і реалізація поняття «інформаційна безпека» є важливим елементом забезпечення стабільності та розвитку сучасного суспільства.

1.2 Правове регулювання забезпечення інформаційної безпеки

Ключовою складовою безпеки інформації є її правовий аспект, який передбачає наявність системи законодавчих актів та гарантій їх ефективності для забезпечення функцій держави у сфері інформаційної діяльності: регулювальної та захисної.

Під правовим регулюванням інформаційної безпеки розуміється система владних нормативних актів, яка дозволяє державі впливати на інформаційні відносини в суспільстві з метою їх організації, закріплення та забезпечення.

Предмет правового забезпечення інформаційної безпеки формується взаємодією суспільних відносин, які стосуються інформації, інформаційної діяльності, інфраструктури та правового статусу суб'єктів інформаційної сфери. Ці відносини належать до об'єктів національних інтересів і пов'язані з проявом загрози безпеці цих об'єктів[20].

Правове забезпечення інформаційної безпеки передбачає дві основні складові: формування та реалізацію правових норм, які відбуваються через правотворчу та правозастосовчу діяльність.

У процесі правотворчої діяльності вирішуються питання формування інформаційної політики, що базується на розвитку інформаційного законодавства України. Це передбачає аналіз стану правової бази у сфері інформаційної діяльності та урахування правозастосовчої практики.

Суть правового забезпечення інформаційної діяльності полягає у створенні та покращенні процесів та систем, що регулюються державою. Основна мета - забезпечення безпеки та ефективності в області інформаційної сфери. Це охоплює дії та діяльність органів публічної влади, які відповідальні за забезпечення інформаційної безпеки[21].

---

[20] Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження // Юридичний вісник. 2021. 1 (58). С. 98.

[21] Сливка М.М., Лук'янова Г.Ю. Правове забезпечення інформаційної безпеки: досвід країн Європейського Союзу // Юридичний науковий електронний журнал. 2021. № 11. С. 515.

Більшість завдань забезпечення інформаційної безпеки покладено на органи публічної влади в Україні. Ці органи відповідають за різноманітні аспекти цієї діяльності:

1) Органи державної виконавчої влади мають завдання забезпечувати інформаційну безпеку у сфері зовнішньої взаємодії. Це включає організацію діяльності об'єктів, які взаємодіють з іншими країнами. Основні функції цих органів можна розділити на кілька типологічних груп, характерних для органів виконавчої влади, зокрема:

- Здійснення правозастосовчої діяльності з реалізації прав і обов'язків суб'єктів приватного права в інформаційній сфері.
- Організація заходів щодо забезпечення інформаційної безпеки та виконання ними основних функцій.
- Захист прав та дотримання законодавства у сфері інформаційної безпеки.
- Організаційно-правове забезпечення дотримання інформаційного законодавства та боротьба з його порушенням [22].
- Управління та координація діяльності органів, відповідальних за інформаційну безпеку.

2) Органи державної виконавчої влади також здійснюють діяльність у сфері внутрішньосистемних об'єктів та проводять внутрішню адміністративну роботу.

3) Проєктна та інноваційна діяльність органів виконавчої влади спрямована на розвиток та формування нових знань у сфері інформаційної безпеки.

4) Органи виконавчої влади забезпечують організаційну структуру та функціонування системи і підрозділів, що відповідають за інформаційну безпеку.

[22] Ільницький М.П. Правове забезпечення інформаційної безпеки у сфері державного управління // Науковий вісник Ужгородського національного університету. Серія: «Право». 2015. Вип. 34. Т. 2. С. 85-86.

5) Деякі функції також виконують інші суб'єкти, які взаємодіють з органами державної виконавчої влади з питань забезпечення інформаційної безпеки та підпадають під регулювання адміністративно-правовими нормами.

6) Правові заходи та система юридичного примусу також використовуються для забезпечення інформаційної безпеки[23].

Загалом, правове забезпечення інформаційної безпеки здійснюється через різноманітні заходи та інструменти, що регулюють відносини у сфері інформаційної діяльності.

Важливо розмежувати поняття інформаційної безпеки як стану динамічної системи та забезпечення інформаційної безпеки як процесу, що дозволяє вирішити протиріччя між організаційно-структурним і функціонально-діяльнісним підходами.

[23] Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження // Юридичний вісник. 2021. 1 (58). С. 100.

1.3 Чинне законодавство в галузі забезпечення інформаційної безпеки в Україні

У Конституції України визначено понад двадцять правових положень, що стосуються забезпечення інформаційної безпеки, що мають найвищу юридичну силу. Серед них ключове значення має право на інформацію та захист державної таємниці.

Основними конституційними нормами у цій галузі є визначення права на отримання інформації та охорону конфіденційної інформації, яка є державною таємницею[24].

Митний кодекс України (статті 186, 214, 344) та Податковий кодекс України (статті 84, 90, 313) також встановлюють норми, що регулюють режим захисту різних видів конфіденційної інформації[2526].

Варто зазначити, що Закон України «Про основи національної безпеки України» визначає дев'ять сфер національної безпеки, серед яких є інформаційна безпека[27]. Він розглядає поняття «безпеки» як стан захищеності життєво важливих інтересів особи, суспільства та держави від загроз ззовні та зсередини. Під життєво важливими інтересами розуміються потреби, чиє задоволення є важливим для існування та прогресивного розвитку особистості, суспільства та держави (стаття 1), а під загрозами безпеки - умови та фактори, які створюють небезпеку для життєво важливих інтересів особистості, суспільства та держави (стаття 3)[28].

[24] Ільницький М.П. Правове забезпечення інформаційної безпеки у сфері державного управління // Науковий вісник Ужгородського національного університету. Серія: «Право». 2015. Вип. 34. Т. 2. С. 85.
[25] Податковий кодекс України: редакція від 01.01.2024 року.
[26] Митний кодекс України: із змінами і доповненнями, внесеними Законами України від 13 квітня 2012 року, N 4652-VI.
[27] Про національну безпеку України: Закон України. Відомості Верховної Ради, № 31, ст.241, 2018.
[28] Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020 // Відомості Верховної Ради України.

Закон «Про захист інформації в інформаційно-комунікаційних системах» є ключовим документом у сфері інформаційної безпеки. У ньому містяться визначення основних термінів, таких як:

1) Інформація - будь-які відомості або дані, незалежно від форми їх подання.

2) Інформаційні технології - процеси та методи пошуку, збору, зберігання, обробки, надання та розповсюдження інформації.

3) Інформаційна система - сукупність інформації, що міститься в базах даних і обробляється інформаційними технологіями та технічними засобами.

4) Власник інформації - особа, яка створила інформацію або має право контролювати доступ до неї.

5) Доступ до інформації - можливість отримання та використання інформації.

6) Конфіденційність інформації - обов'язок не передавати інформацію третім особам без згоди її власника.

7) Надання інформації - дії, спрямовані на передачу інформації певному колу осіб.

8) Поширення інформації - передача інформації невизначеному колу осіб.

9) Електронне повідомлення - інформація, передана чи отримана через інформаційно-телекомунікаційну мережу.

10) Документована інформація - інформація, зафіксована на матеріальному носії з реквізитами, що дозволяють ідентифікувати її.

11) Оператор інформаційної системи - особа або організація, яка відповідає за експлуатацію інформаційної системи [29].

Зазначений закон встановлює правила захисту інформації та визначає відповідальність за порушення цих правил.

[29] Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.94, № 81/94-ВР: із змінами, внесеними від 16.12.2020, № 1089-IX // Відомості Верховної Ради України.

Правове регулювання в сфері захисту інформації, як передбачено відповідним законодавством, базується на наступних принципах:

1) Забезпечення свободи пошуку, отримання, передачі, виробництва та розповсюдження інформації за будь-якими законними засобами.

2) Встановлення обмежень доступу до інформації лише законом.

3) Забезпечення відкритості інформації про діяльність державних та місцевих органів самоврядування та вільний доступ до неї, за винятком випадків, встановлених законом.

4) Гарантування безпеки України у сфері створення, експлуатації та захисту інформаційних систем, що містять конфіденційну інформацію.

5) Забезпечення достовірності інформації та її своєчасного надання.

6) Забезпечення недоторканості приватного життя та заборона збору, зберігання, використання та розповсюдження інформації про приватне життя особи без її згоди.

7) Заборона встановлення переваг застосування певних інформаційних технологій перед іншими, якщо обов'язковість застосування певних технологій не встановлена законом[30].

На жаль, на законодавчому рівні питання системи інформаційної безпеки ще не розв'язано системно. Навіть нова Доктрина інформаційної безпеки України, яка готувалася в умовах гібридної агресії Російської Федерації, не вирішує всі проблеми та не орієнтує на необхідність їх законодавчого врегулювання. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, зокрема протидія руйнівному інформаційному впливу РФ в умовах гібридної війни[31].

Доктрина визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями та пріоритети державної політики в цій сфері. Її правовою основою є Конституція України, закони України, Стратегія

[30] Там само.

[31] Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 13.02.2017 №47 // Відомості Верховної Ради України.

національної безпеки України, затверджена Указом Президента від 26 травня 2015 року № 287, а також міжнародні договори, ратифіковані Верховною Радою України.

Я повністю підтримую думку О. Довганя, який правильно вказує на необхідність вирішення питання розробки нормативного акту, такого як закон, що однозначно визначить поняття та категорії, пов'язані з інформаційною безпекою, державну політику забезпечення цієї безпеки, об'єкти та суб'єкти її забезпечення, а також правові аспекти відповідальності відомств, що залучені до цієї сфери. Такий закон повинен визначити механізми координації діяльності органів та відомств для реагування на виклики та загрози національній безпеці в інформаційній сфері, а також порядок взаємодії між ними[32].

Щодо цього, на засіданні РНБО України 17 січня 2018 року члени РНБО обговорили та підтримали проєкт Закону України «Про національну безпеку України», який був розроблений у співпраці з експертами НАТО, США та Європейського Союзу. На жаль, за результатами аналізу цього проєкту можна зробити висновок, що він не відповідає вимогам нормативно-правової техніки і містить деякі недоліки.

Тому актуальною стає потреба у розробці та прийнятті Закону України «Про інформаційну безпеку України», який має стати основою для ефективної стратегії забезпечення інформаційної безпеки. Цей закон має містити чіткі визначення основних категорій у сфері інформаційної безпеки, а також забезпечити правову базу для взаємодії суб'єктів забезпечення цієї безпеки.

Створення належних умов для забезпечення державної політики, спрямованої на захист національних цінностей та втілення національних інтересів України, а також забезпечення безпеки особи, суспільства і держави від зовнішніх та внутрішніх загроз в інформаційній сфері, потребує створення сучасних та ефективних механізмів забезпечення інформаційної безпеки.

[32] Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці в інформаційній сфері // Вісник Національної академії правових наук України. 2014. № 3 (78). С. 43-52.

Складна ситуація на воєнно-політичному, оперативно-стратегічному та економічному рівнях, викликана збройною агресією Російської Федерації проти України, справила небезпечний вплив на інформаційний простір.

Тому, надзвичайно важливим стає як доктринальне, так і нормативне визначення ключової категорії – «система інформаційної безпеки», оскільки інформаційна безпека є складною системою, що впливає на різні рівні через зовнішні та внутрішні фактори, такі як політична та внутрішньополітична обстановка, рівень розвитку інформаційно-комунікаційних технологій та інші.

Таким чином, українське законодавство у сфері інформаційної безпеки охоплює норми конституційного, адміністративного, цивільного, кримінального, трудового та інших галузей правового регулювання.

У методологічному плані важливо не лише перерахувати складові системи інформаційної безпеки, а й узгодити ці явища з конкретними поняттями.

Подальший розвиток інформаційного законодавства у сфері забезпечення інформаційної безпеки обумовлений приведенням законодавства у відповідність із ратифікованою Україною Європейською Конвенцією про захист фізичних осіб при автоматизованій обробці персональних даних та у розробці та ухваленні Закону України «Про інформаційну безпеку України» як основного закону, який регулюватиме питання інформаційної безпеки[33].

Отже, Україна, як держава, що активно інтегрується у світовий інформаційний простір, стикається з численними викликами в сфері інформаційної безпеки.

Чинне законодавство України в галузі інформаційної безпеки має на меті забезпечити захист національних інтересів, стабільність функціонування державних і суспільних інформаційних систем, а також права і свободи громадян.

[33] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: ратифікація від 06.07.2010, N 2438-VI.

РОЗДІЛ ІІ. ОСНОВНІ НАПРЯМКИ РОЗВИТКУ ПРАВОВОГО РЕГУЛЮВАННЯ В ОБЛАСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ ОРГАНІВ ВЛАДИ ТА УПРАВЛІННЯ

2.1 Інформаційне забезпечення державної політики у сфері забезпечення інформаційної безпеки

Система інформаційного забезпечення державної політики у сфері забезпечення інформаційної безпеки відіграє ключову роль у координації управління з метою забезпечення сталого розвитку та захисту національних інтересів в інформаційній сфері від внутрішніх та зовнішніх викликів і загроз. Вона являє собою складну мережу державних органів, а також інших уповноважених суб'єктів, які активно беруть участь у здійсненні інформаційного супроводу забезпечення державної політики, реагуючи на виклики та впроваджуючи нормативно-правові акти, що регулюють відповідні суспільні відносини[34].

При проведенні цього дослідження слід розглядати державну політику в галузі забезпечення інформаційної безпеки в широкому контексті, оскільки інформаційна безпека в сучасному інформаційному суспільстві пронизує всі аспекти життєдіяльності особистості, суспільства та держави. Вона стає невід'ємною складовою кожного аспекту сучасного життя, вимагаючи комплексного та системного підходу до забезпечення безпеки інформаційного простору.

Державна політика у сфері використання інформаційних технологій у державному управлінні спрямована на забезпечення координації діяльності органів у структурі державної влади щодо створення державних інформаційних систем, ресурсів і надання громадських послуг, а також на підвищення ефективності бюджетних витрат у цій сфері. Політика в цьому напрямку має

[34] Новицька Н.Б. Правове забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави. 2009. № 1. С. 46.

сприяти розвитку інформаційного суспільства та покращенню якості життя громадян[35].

Інформаційне забезпечення державної політики має здійснюватися на основі ряду ключових принципів, серед яких варто виділити такі:

1) Відкритість державної політики: усі ключові заходи, пов'язані з державною політикою, повинні бути відкрито обговорені з громадськістю, і держава має враховувати громадську думку при формуванні стратегій та програм.

2) Рівність інтересів усіх учасників: всі суб'єкти, які беруть участь у формуванні державної політики, повинні мати рівні можливості впливу на процеси прийняття рішень.

3) Системність: при впровадженні нових заходів та змінах у стані одного об'єкта регулювання необхідно ураховувати їх вплив на інші аспекти та на загальний стан суспільства.

4) Соціальна орієнтація: основні напрямки державної політики мають сприяти задоволенню соціальних потреб і інтересів громадян.

5) Пріоритетність права: розвиток та застосування правових та економічних механізмів має бути переважаючим перед адміністративними рішеннями[36].

Основними завданнями системи інформаційного забезпечення державної політики є:

По-перше, ефективне формування та використання національних інформаційних ресурсів та забезпечення широкого, вільного доступу до них. Це означає створення і підтримку інформаційних баз даних, розробку інформаційних порталів та інтерфейсів, які сприяють ефективному обміну даними та доступу до них для різних користувачів.

---

[35] Конах В.К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США): автореф. дис ... канд. політ. наук: спец. 21.01.01 / Нац. ін-т стратег. дослідж. Київ, 2005. С. 3-4.

[36] Орлов П.І. Правове забезпечення інформаційної безпеки // Вісник Харківського національного університету внутрішніх справ. 2001. Вип. 15. С. 96-97.

По-друге, забезпечення громадян суспільно значущою інформацією та розвиток незалежних засобів масової інформації. Це передбачає створення умов для вільного розповсюдження інформації, захист прав на свободу слова та доступ до об'єктивної та неперекрученої інформації.

По-третє, створення необхідної нормативно-правової основи формування системи інформаційного забезпечення державної політики. Це означає розробку та впровадження законів, нормативних актів та політичних стратегій, які регулюють інформаційні процеси в державі та забезпечують їх відповідність сучасним стандартам та вимогам[37].

Однорідні, суттєво взаємопов'язані компоненти системи інформаційного забезпечення державної політики мають консолідуватись у єдині загальнодержавні системи та структури, що об'єднують інформаційний простір держави у єдине ціле для забезпечення формування державної внутрішньої та зовнішньої політики.

Основні напрями державної політики України реалізуються через систему державних органів, що має сприяти координації управління. Державні органи, органи місцевого самоврядування відповідно до своїх повноважень беруть участь у розробці та реалізації цільових програм застосування інформаційних технологій, а також створюють інформаційні системи та забезпечують доступ до інформації, що в них міститься, державною мовою України.

Багато в чому завдяки діяльності системи інформаційного забезпечення державної політики вдалося досягти громадської підтримки заходів щодо реалізації національних проектів, проведення адміністративної реформи, а також забезпечити певний рівень довіри населення до діяльності державних органів та розпочати створення системи державних гарантій реалізації прав людини та громадянина на отримання достовірної та об'єктивної інформації про діяльність державних органів[38].

---

[37] Довгань О.Д., Ткачук Т.Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс // Інформація і право. 2018. № 2 (25). С. 75.

[38] Наливайко Л.М. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект // Вісник Запорізького державного університету. Серія: «Юридичні науки». 2003. № 1. С. 62-63.

Водночас слід визнати обґрунтованою критику недостатньо широкого інформування державними органами громадян про свої дії, що становлять значний суспільний інтерес, особливо на етапі підготовки рішень, виконання прийнятих рішень. Зберігається недостатній рівень координації діяльності об'єктів інформаційного супроводу державної політики.

Правові норми, що регулюють правове забезпечення державної політики та державне регулювання у сфері застосування інформаційних технологій, визначено в законодавстві України, зокрема в Законі «Про захист інформації в інформаційно-комунікаційних системах».

Основними напрямами діяльності, що передбачені законом, є розвиток інформаційних систем різного призначення для задоволення потреб громадян, організацій, державних органів та органів місцевого самоврядування у доступі до інформації та взаємодії між ними. Також надається увага створенню умов для ефективного використання інформаційно-телекомунікаційних мереж, включаючи Інтернет та інші подібні системи зв'язку[39].

Законодавство регулює ці питання з метою забезпечення безпеки, ефективності та доступності інформації для всіх суб'єктів взаємодії в інформаційно-комунікаційному просторі.

Основною метою створення системи інформаційного забезпечення державної політики та використання інформаційних технологій у діяльності федеральних органів державної влади є підвищення ефективності механізмів державного управління. Це досягається через створення загальної інформаційно-технологічної інфраструктури, яка включає державні інформаційні системи та ресурси, а також засоби, що забезпечують їх функціонування та взаємодію між собою, населенням та організаціями. Це допомагає у наданні державних послуг та реалізації прав громадян у сфері інформації.

---

[39] Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.94, № 81/94-ВР // Відомості Верховної Ради України.

Основними напрямами державної політики у інформаційній сфері можна назвати наступні:

1) Забезпечення умов для ефективної реалізації та захисту конституційних прав та свобод людини в інформаційній сфері.

2) Створення політичних, економічних, правових та інших засад побудови інформаційного суспільства.

3) Розвиток національної інформаційної інфраструктури та забезпечення економічних та правових умов для розвитку ринку та інформаційних технологій.

4) Сприяння застосуванню інформаційних технологій у державному управлінні, економіці, обороні, охороні здоров'я, освіті, екології тощо.

5) Забезпечення рівноправної інтеграції країни до глобального інформаційного простору та дотримання міжнародних договорів та угод у інформаційній сфері[40].

Однією з найважливіших функцій держави є зовнішньополітична діяльність, яка передбачає взаємодію на офіційному рівні з іншими країнами та міжнародними організаціями. Для досягнення цієї мети необхідно вдосконалювати систему інформаційного забезпечення державної політики. Вона повинна базуватися на чіткій структурі та ролі органів державної влади. Проте на сьогоднішній день роль координуючого органу у цій сфері визначена недостатньо чітко.

Нормативно-правове забезпечення, що регламентує питання взаємодії громадян та організацій з державними інститутами, також пов'язане з реалізацією державної політики. Воно вимагає забезпечення інформаційної безпеки та повинно ґрунтуватися на системності, усуненні прогалин та врегулюванні ключових питань, що стосуються права на інформацію та доступу до неї.

[40] Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження // Юридичний вісник. 2021. 1 (58). С. 97.

Окрім основних законодавчих та інших нормативних актів, які регулюють структуру системи органів влади та встановлюють правила та порядок роботи, для ефективного інформаційного забезпечення державної політики необхідно приймати відповідні управлінські рішення. Це можуть бути як адміністративні, так і нормативно-правові акти, спрямовані на формування зв'язків та забезпечення взаємодії між різними гілками та рівнями влади [41].

Реалізація державної політики у сфері формування державних інформаційних ресурсів є невід'ємною складовою процесу становлення інформаційного суспільства. Цей процес повинен бути адаптивним та орієнтованим на впровадження сучасних інформаційних технологій, враховуючи активне використання Інтернету та інших електронних платформ.

Для досягнення цієї мети важливо забезпечити створення, обробку, обмін та надання інформаційних ресурсів у електронній формі, завірити їхню достовірність та цілісність, а також забезпечити права громадян та організацій на доступ до інформації. Крім того, важливо зміцнити контроль за інформаційною безпекою та використовувати криптографічні засоби для захисту інформаційних ресурсів під час їх передачі.

Не менш важливою є роль кадрового забезпечення, яке потребує визначення та прогнозування потреб у фахівцях у цій галузі. Підвищення якості підготовки наукових та технічних кадрів сприятиме ефективнішому впровадженню сучасних інформаційних технологій та забезпечить успішне функціонування системи інформаційного забезпечення державної політики.

Одним із пріоритетних напрямів державної політики у сфері забезпечення інформаційної безпеки є вдосконалення механізмів правового регулювання суспільних відносин. Зростаюча важливість цієї сфери вимагає системного підходу до розвитку законодавства, яке має базуватися на загальноправових та галузевих принципах[42].

---

[41] Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні // Право і суспільство. 2012. № 3. С. 135-136.

[42] Орлов П.І. Правове забезпечення інформаційної безпеки // Вісник Харківського національного університету внутрішніх справ. 2001. Вип. 15. С. 98.

Розвиток законодавства в галузі інформаційної безпеки передбачає створення системи правил, що забезпечують дотримання законності, справедливості та захисту прав громадян. Така система має враховувати важливі аспекти, такі як гуманізм, демократизм та міжгалузеві зв'язки.

Для успішної реалізації державної політики у цій сфері важливо визначити основні фактори, що впливають на формування системи законодавства та розвиток інформаційно-комунікаційної інфраструктури. Це охоплює не лише правове поле, а й науково-технічний аспект, а також виробничий комплекс інформаційної індустрії та освітні програми для професійних кадрів.

З метою забезпечення ефективного інформаційного забезпечення державної політики важливо визначити об'єкти захисту. Це включає в себе інформацію та права на неї, захист громадян і суспільства від негативного впливу інформації та збереження прав на інформаційні системи.

Такий комплексний підхід дозволяє створити цілісну систему законодавства, яка враховує всі аспекти забезпечення інформаційної безпеки та сприяє реалізації стратегічних завдань держави в цій сфері.

Звісно ж, що у галузі нормативно-правового забезпечення безпеки інформаційно-телекомунікаційних систем та мереж існують важливі напрями регулювання, які визначаються для ефективної реалізації державної інформаційної політики. Такі напрями включають:

1) Захист прав особистості, інтересів суспільства та держави під час використання інформаційно-телекомунікаційних систем та мереж.

2) Захист інформації в інформаційно-телекомунікаційних системах та мережах.

3) Забезпечення стійкого функціонування інформаційно-телекомунікаційних систем та мереж.

4) Розвиток міжнародного співробітництва у сфері безпеки функціонування глобальних інформаційних систем та мереж.

5) Система інформаційного забезпечення державної політики у цій галузі включає в себе різноманітні державні органи та інші суб'єкти, які спільно здійснюють інформаційний супровід та реалізацію нормативно-правових актів[43].

Крім того, у галузі нормативно-правового забезпечення інформаційної безпеки важливо враховувати такі аспекти:

1) Правова рівність усіх учасників інформаційної взаємодії, незалежно від їхнього соціального, політичного та економічного статусу.

2) Гарантування конституційного права громадян на вільний доступ до інформації та її обмін.

Ці напрями регулювання є важливими складовими у формуванні сучасної системи забезпечення інформаційної безпеки, яка сприяє стабільності та розвитку суспільства[44].

Ефективне інформаційне забезпечення передбачає створення комплексної системи заходів, спрямованих на захист інформації, прав особистості та інтересів суспільства.

Для досягнення цієї мети необхідно:

1) Розвивати нормативно-правову базу, яка гарантує права громадян на доступ до інформації та забезпечує конфіденційність та цілісність даних у цифровому середовищі.

2) Забезпечувати стійке функціонування інформаційних систем та мереж шляхом впровадження сучасних технологій захисту від кіберзагроз та кібератак.

3) Зміцнювати міжнародне співробітництво у сфері інформаційної безпеки для вирішення спільних викликів та загроз.

---

[43] Там само. С. 98-99.

[44] Алямкін Р.В. Правове забезпечення національної інформаційної безпеки // Наукові записки Інституту законодавства Верховної Ради України. 2013. № 4. С. 94-95.

4) Забезпечувати доступність та прозорість інформації для громадян, підвищуючи рівень їхньої обізнаності та захищаючи їх від дезінформації та маніпуляцій[45].

Підсумовуючи інформаційне забезпечення державної політики у сфері забезпечення інформаційної безпеки є важливою складовою сучасного управління та функціонування держави. Це охоплює широкий спектр заходів та стратегій, спрямованих на захист інформації та забезпечення безпеки інформаційних ресурсів на всіх рівнях суспільства.

На першому рівні інформаційне забезпечення полягає в захисті особистих даних громадян. Це охоплює прийняття та виконання відповідних законодавчих актів, які гарантують конфіденційність та безпеку особистої інформації кожного громадянина.

На другому рівні інформаційне забезпечення включає заходи щодо захисту інформаційних систем та мереж в рамках державних установ та організацій. Це передбачає розробку та впровадження технічних та організаційних заходів, спрямованих на запобігання кібератакам та злому інформаційних ресурсів.

На третьому рівні інформаційне забезпечення передбачає захист національних інформаційних систем від зовнішніх загроз. Це включає в себе розробку та впровадження стратегій кібербезпеки, співпрацю з міжнародними партнерами та організаціями для обміну інформацією та координації дій у випадку кібератак.

[45] Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні // Підприємництво, господарство і право. 2019. № 9. С. 105-106.

2.2 Заходи щодо реалізації концептуальних та доктринальних документів забезпечення інформаційної безпеки

На основі аналізу законодавства щодо інформаційної безпеки стає очевидним, що потрібне упорядкування законодавства у цій сфері. Важливо визначити принципи державної політики та розробити концепцію для подальшого розвитку та вдосконалення законодавства.

Дотримання принципу законності – один із основних принципів права, що вимагає від державних органів чітко дотримуватися нормативно-правових актів у вирішенні конфліктів у сфері інформації.

Особливістю правового забезпечення інформаційної безпеки є необхідність збалансувати інтереси особистості, суспільства та держави в цій сфері. Це передбачає закріплення пріоритету цих інтересів у різних сферах життєдіяльності та використання механізмів громадського контролю.

Забезпечення конституційних прав і свобод громадян у сфері інформаційної безпеки є одним із найважливіших завдань держави[46].

Нажаль, відсутність регулювання в сфері інформатизації та інформаційної безпеки, формування та використання державних інформаційних ресурсів, а також захисту інтересів користувачів і власників інформаційних ресурсів від потенційних загроз може мати серйозні негативні наслідки.

Необхідно розробити концептуальні підходи для забезпечення захищеності від внутрішніх та зовнішніх загроз у сфері інформації. Серед них можуть бути такі аспекти, як «інформаційна зброя», вплив інформації на психіку та поведінку людини, а також використання глобальних інформаційних систем та мереж.

Стан захищеності, який визначається рівнем інформаційної безпеки, є динамічним і вимагає постійного вдосконалення в умовах сучасного «інформаційного століття». Це обумовлено зростанням загроз, зміною

[46] Алямкін Р.В. Правове забезпечення національної інформаційної безпеки // Наукові записки Інституту законодавства Верховної Ради України. 2013. № 4. С. 92.

технологій та їхньою зловживанням, що потребує відповідного реагування та просування вперед із заходами забезпечення безпеки в цій сфері.

Для забезпечення інформаційної безпеки важливий розвиток та вдосконалення законодавства в цій сфері. Це потребує комплексного, міждисциплінарного та системного підходу, який включає науково-теоретичні та правові дослідження особливостей суспільних відносин у сфері інформації, нові виклики та загрози, а також розробку концепційних документів.

Необхідно розглянути внесення змін до чинних нормативних актів, включаючи закони, що регулюють питання власності в інформаційній сфері та охорони прав на об'єкти інтелектуальної власності.

У правовому регулюванні суспільних відносин у мережі інформаційних технологій існують суттєві прогалини. Наприклад, необхідно вдосконалити механізми: розподілу компетенції державних органів у формуванні інформаційних ресурсів, ліцензування та сертифікації інформаційних систем та технологій, захисту авторських прав та гарантії права на інформацію.

Вирішення цих питань вимагає внесення відповідних законодавчих змін та ретельного аналізу їхнього впливу на суспільство та інформаційну безпеку[47].

З розвитком інформаційного суспільства та настанням нових суспільних відносин виникає потреба в адекватному правовому регулюванні. Ця проблема набуває особливої гостроти і соціальної значущості. Правова база для створення єдиного інформаційного простору в Україні та будівництва інформаційного суспільства має сприяти гармонійному розвитку інформаційних ресурсів, послуг та засобів їх виробництва.

Важливість проблеми вироблення концептуальних підходів до розвитку законодавства в інформаційній сфері не може бути недооцінена, оскільки норми законів цієї галузі суттєво впливають на якість регулювання відносин між суб'єктами у всіх сферах життя країни. Отже, важливо забезпечити розвиток законодавства, яке враховує сучасні виклики та потреби інформаційного

[47] Ільницький М.П. Правове забезпечення інформаційної безпеки у сфері державного управління // Науковий вісник Ужгородського національного університету. Серія: «Право». 2015. Вип. 34. Т. 2. С. 85-86.

суспільства, забезпечуючи таким чином стабільність і безпеку національної інформаційної інфраструктури.

Отже, заходи щодо реалізації концептуальних та доктринальних документів забезпечення інформаційної безпеки виявляються критично важливими для забезпечення стійкості та безпеки інформаційного середовища. Ці заходи потребують системного та комплексного підходу, що охоплює не лише розробку та прийняття відповідних стратегій і політик, але й їхню ефективну реалізацію на практиці.

Широке ознайомлення громадськості з важливістю заходів забезпечення інформаційної безпеки, спільна робота різних галузей та органів влади, а також постійне оновлення та адаптація концептуальних документів до сучасних викликів і загроз є ключовими компонентами успішної реалізації цих заходів.

Такий підхід дозволить створити більш безпечне та стійке інформаційне середовище, сприятиме розвитку інформаційного суспільства та забезпечить захист прав індивідів та інтересів суспільства в цифровій епохі.

2.3 Система міжнародної інформаційної безпеки

У зв'язку з глобалізацією інформаційних процесів і поширенням інформації через кордони, виникає необхідність в дослідженні проблем створення міжнародної системи інформаційної безпеки. Така система має враховувати нові виклики та загрози, що виникають у сучасній інформаційній сфері, а також користуватися накопиченим міжнародним досвідом у цій області.

Рада Європи, Європейський Союз, ООН та ШОС (Шанхайська організація співробітництва) є активними учасниками у формуванні міжнародних стандартів інформаційної безпеки. Наприклад, Рада Європи вже з кінця 1993 року розпочала роботу над побудовою інформаційного суспільства та прийняла рішення про створення умов для вільного доступу до інформації, забезпечуючи при цьому захист прав особистості та суспільства.

У той же час, ООН проводить переговори з приводу правового режиму міжнародної інформаційної безпеки, спрямовуючи зусилля на визначення міжнародно-правового режиму та понять у цій області. Україна також активно вносить свої пропозиції та ініціативи в цей процес, надсилаючи відповідні пропозиції до Секретаріату ООН.

Такий міжнародний підхід до забезпечення інформаційної безпеки відображає важливість співпраці та обміну досвідом між країнами з метою створення більш безпечного та стійкого інформаційного середовища на світовому рівні[48].

Ефективне протистояння сучасним викликам та загрозам безпеці в інформаційній сфері вимагає вжиття скоординованих заходів на всіх рівнях - від двостороннього до багатостороннього міжнародного співробітництва. Однак ключовою складовою успішної стратегії буде вдосконалення міжнародної

[48] Скалацький В. М. Інформаційне суспільство: сучасні теорії та моделі (соціальнофілософський аналіз): дис.: 09.00.03. Київ: Київ. нац. ун-т ім. Тараса Шевченка, 2006. С. 150-152.

правової бази співпраці та розробка єдиного понятійного апарату у сфері забезпечення міжнародної інформаційної безпеки.

Розвиток світового співтовариства в напрямку глобального інформаційного суспільства вимагає комплексного правового регулювання суспільних відносин у сфері забезпечення інформаційної безпеки. Цей підхід відображений у міжнародних правових актах і стає ключовим фактором координації зусиль держав у побудові системи міжнародної інформаційної безпеки.

Актуальність міжнародного співробітництва у цій галузі підтверджується досвідом роботи Шанхайської організації співробітництва. Ініціативи цієї організації, спрямовані на вироблення узгоджених понять та розробку міжнародних правових актів, свідчать про необхідність спільних зусиль у забезпеченні міжнародної інформаційної безпеки.

Згідно з Заявою глав держав-членів Шанхайської організації співробітництва від 15 червня 2006 року, було прийнято рішення про створення Групи експертів держав-членів ШОС з міжнародної інформаційної безпеки (МІБ). Ця ініціатива мала на меті розробити план дій для держав-членів ШОС у сфері інформаційної безпеки та визначити шляхи вирішення проблем у всіх її аспектах.

Відповідно до рішення, прийнятого главами держав 16 серпня 2007 року, міжнародна Група експертів розробила План дій щодо забезпечення міжнародної інформаційної безпеки[49]. Цей план передбачав співпрацю за різними напрямами з метою створення системи міжнародної інформаційної безпеки:

1) Вироблення єдиного понятійного апарату для підвищення ефективності взаємодії в галузі МІБ на просторі ШОС та забезпечення сумісності законодавства держав-членів.

2) Аналіз існуючих та потенційних загроз у галузі МІБ та вироблення пропозицій щодо застосування адекватних заходів протидії їм.

[49] Сливка М.М., Лук'янова Г.Ю. Правове забезпечення інформаційної безпеки: досвід країн Європейського Союзу // Юридичний науковий електронний журнал. 2021. № 11. С. 515.

3) Розробка механізмів моніторингу загроз та координації дій щодо забезпечення інформаційної безпеки на просторі ШОС.

4) Вивчення та порівняння національних законодавств у сфері забезпечення інформаційної безпеки.

5) Дослідження міжнародно-правового регулювання та стану міжнародно-правової бази сфери МІБ.

6) Участь у міжнародних організаціях та форумах, проведення консультацій експертів з правових питань забезпечення інформаційної безпеки.

7) Розробка та реалізація заходів довіри між державами-членами ШОС у сфері забезпечення інформаційної безпеки.

8) Вивчення можливостей розробки та укладання міжнародних угод про співробітництво у цій сфері.

Ці заходи спрямовані на покращення співпраці та забезпечення міжнародної інформаційної безпеки на просторі ШОС[50].

Право на доступ до інформації, як його визначають міжнародні документи з прав людини, не є новим для суспільства. Це скоріше вияв традиційних свободи думки та слова в міжнародному інформаційному обміні. Засновані на цих принципах принципи стали основою принципу вільного потоку інформації, який залишається домінуючим у світі відносин.

У сфері міжнародної інформаційної безпеки важливість законодавчого регулювання визначена основними міжнародними документами, які стали пріоритетними для України у сфері розвитку інформаційного законодавства.

Особлива увага приділяється участі в міжнародних дослідницьких проєктах, розробці міжнародних стандартів та гармонізації національних систем стандартизації. Такий підхід відображає мету державної політики в галузі міжнародної інформаційної безпеки, спрямованої на підтримку миру та стабільності.

[50] Там само. С. 515-516.

Формування системи міжнародної інформаційної безпеки потребує створення механізмів для забезпечення довіри в сфері використання інформаційних технологій, а також міжнародної системи розслідування злочинів, пов'язаних із кібертероризмом[51].

Дискусії про анонімність в Інтернеті та її наслідки, такі як порушення авторських прав та злочини, тривають. Навіть при підтримці принципу анонімності, який зазначений у Декларації про свободу комунікацій в Інтернеті Ради Європи, держави можуть застосовувати заходи для виявлення злочинців відповідно до свого національного та міжнародного законодавства[52].

Розробка механізмів для обмеження анонімності у транскордонному електронному обміні та його використання для забезпечення міжнародної інформаційної безпеки потребує складних технічних, організаційних, політичних та міжнародно-правових заходів. Важливо забезпечити надійну ідентифікацію користувачів та перевести міждержавну співпрацю при розслідуванні порушень міжнародної інформаційної безпеки у сферу міжнародного права.

У будівництві інформаційного суспільства вирішення цих проблем є ключовим, оскільки воно є фундаментом для забезпечення міжнародної інформаційної безпеки, запобігання шкоді інфраструктурі держави, впливу на економіку та політику, а також боротьби з тероризмом та екстремізмом.

Отже, система міжнародної інформаційної безпеки в сучасному світі потребує вдосконаленого та широкого підходу, який охоплює координацію дій не лише держав, але й міжнародних організацій та інших учасників світової спільноти. Величезне значення має розвиток та зміцнення міжнародного співробітництва у цій сфері, що передбачає активну роботу над впровадженням стандартів та механізмів, спрямованих на запобігання загрозам інформаційної безпеки.

---

[51] Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні // Підприємництво, господарство і право. 2019. № 9. С. 102-103.

[52] Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003.

Розв'язання цих складних завдань вимагає не лише технічних та організаційних заходів, але й підтримки на рівні політичної волі та міжнародно-правового регулювання. Це означає, що країни повинні спільно працювати над створенням ефективної системи обміну інформацією, співпрацювати у вирішенні спільних проблем та розробляти міжнародні стандарти і норми, спрямовані на забезпечення стабільності та безпеки в інформаційному просторі.

Такий підхід відкриває можливості для спільних ініціатив та проектів, спрямованих на покращення безпеки в інтернеті, захист особистих даних та боротьбу з кіберзлочинністю. Крім того, це сприяє зміцненню міжнародних відносин та підвищенню довіри між країнами.

2.4 Міжнародний досвід правового регулювання забезпечення інформаційної безпеки

Формування якісної системи інформаційної безпеки, яка б відповідала нагальним потребам України і сучасним вимогам, потребує використання позитивних здобутків країн-учасниць ЄС в інформаційній сфері.

З огляду на геополітичне положення України її провідним орієнтиром мають стати передусім країни Центральної Європи, адже саме вони є успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства шляхом створення розвиненої інфраструктури інформаційних технологій з унікально високим рівнем доступу населення до них, випереджаючи за цим показником інші країни світу[53].

Серед багатьох міжнародних законодавчих актів чітко простежується теза, що інформаційна та мережева безпека охоплює здатність мережі або системи стійко протистояти різним видам загроз і зловмисних дій, спрямованих на порушення доступності, цілісності і конфіденційності інформації та послуг. Забезпечення безпеки полягає у забезпеченні доступності, ідентифікації, цілісності та конфіденційності інформації.

Законодавчі акти, які визначають інформаційну безпеку, часто встановлюють заходи для захисту інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, поширення, модифікації або знищення. Наприклад, у Законі США «Про управління інформаційною безпекою» інформаційна безпека охарактеризована як захист інформації та інформаційних систем від різних загроз, а також забезпечення цілісності, конфіденційності і доступності інформації[54].

Для багатьох країн зарубіжжя характерний підхід до проблеми інформаційної безпеки з урахуванням таких ключових понять, як

[53] Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства // Науковий вісник Ужгородського національного університету. Серія «Право». 2017. Вип. 43. Т. 1. С. 35.
[54] Скалацький В. М. Інформаційне суспільство: сучасні теорії та моделі (соціальнофілософський аналіз): дис.: 09.00.03. Київ: Київ. нац. ун-т ім. Тараса Шевченка, 2006. С. 151-152.

«автентичність», «доступність», «цілісність» та «конфіденційність». Наприклад, Закон США «Про захист інформації» від 1998 року відображає аналогічні принципи, які містить Закон 1984 року відповідно до Директиви 95/46 Європейського Союзу щодо захисту прав на персональні дані. Ці закони обмежують використання персональних даних та регулюють доступ до облікових записів, ведених як державними установами, так і приватними компаніями[55].

Питання недоторканності приватного життя також регулюються іншими законодавчими актами США, включаючи закони, що стосуються ведення медичних записів, обліку споживчих кредитів та інші. Наприклад, Закони «Про реабілітацію правопорушників» 1974 року та «Про телекомунікації» 1984 року також враховують аспекти приватності та захисту інформації[56].

Серед найстаріших законодавчих актів можна відзначити Закон «Про свободу друку» 1766 року, прийнятий у Швеції, який гарантує право громадян на доступ до інформації про діяльність державних органів. Цей закон зараз охоплює всі типи документів, включаючи електронні.

У Нідерландаї, Іспанії, Португалії, Австрії, Угорщині, Естонії, Бельгії та Румунії, право громадян на доступ до офіційної інформації забезпечено на конституційному рівні. В той же час, у Франції, Греції та Італії ці права закріплені в законах. Процес удосконалення законодавства в цій сфері триває в країнах, таких як Велика Британія, Німеччина, Естонія, Молдова, Польща та інші.

Слід відзначити, що у Швеції та Фінляндії існують обмеження прав на доступ до урядової інформації, що визначено законодавчо. На сьогоднішній день у багатьох зарубіжних країнах, а також в Україні, активно розробляються та впроваджуються концепції електронного уряду, що базується на використанні

[55] Сливка М.М., Лук'янова Г.Ю. Правове забезпечення інформаційної безпеки: досвід країн Європейського Союзу // Юридичний науковий електронний журнал. 2021. № 11. С. 515.
[56] Конах В.К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США): автореф. дис ... канд. політ. наук: спец. 21.01.01 / Нац. ін-т стратег. дослідж. Київ, 2005. С. 5-6.

інформаційних технологій для створення державних інформаційних ресурсів та забезпечення доступу до інформації про діяльність державних органів влади, відкритих даних (це практикується у США, Сінгапурі, Австралії, Новій Зеландії та інших країнах)[57].

У Австрії, наприклад, громадянам законодавчо гарантовано доступ до нормативно-правової бази, при цьому інформація знаходиться у володінні державного сектору, а не комерційних структур (існує плата за копіювання та розповсюдження). Таким чином, аналіз зарубіжного досвіду правового регулювання питань доступу до інформації свідчить про різноманітність підходів та тенденцій у забезпеченні інформаційної безпеки.

Значна частина законодавства та інших нормативних актів у цій сфері в багатьох країнах стосується електронної торгівлі та використання електронних підписів. Наприклад, це включає такі закони, як Закон Канади «Про електронні угоди» 1999 року, Федеральний закон США «Про електронні підписи в міжнародній і внутрішній торгівлі» 2000 року, Закон Ірландії «Про електронну торгівлю» 2000 року, Закон Іспанії «Про послуги інформаційного суспільства та електронну торгівлю» 2002 року, Закон Південної Кореї «Про електронну торгівлю» 2001 року, Закон Таїланду «Про електронні угоди і електронний підпис» 2002 року тощо[58].

Детальний аналіз ситуації у правовому регулюванні інформаційної безпеки в зазначених зарубіжних країнах свідчить про широке впровадження нормативно-правових актів, спрямованих на захист інформації, інформаційної техніки та технологій. Більшість держав вже мають закони, що регулюють створення та захист інформаційних мереж та встановлюють загальні умови використання ліній зв’язку та комунікаційних послуг.

Особливу увагу у правовому забезпеченні інформаційної безпеки привертають питання захисту персональних даних, які регламентуються в

[57] Почепцов Г. Г. Інформаційна політика: навч. посіб. Київ: Знання, 2006. С. 130.

[58] Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України: дис. ... д-ра політ. наук: спец. 23.00.02. / Одес. нац. юрид. акад. Одеса, 2005. С. 131.

багатьох країнах. Наприклад, в Іспанії ще у 1999 році був ухвалений Органічний закон «Про захист персональних даних», що визначає загальнодоступні джерела інформації, такі як списки кандидатів на посади, телефонні довідники та інші.

Україна також досягла важливого кроку, завершивши процедуру ратифікації Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних 1981 року. Це стало важливим кроком на шляху до повноцінної участі країни в ініціативах Ради Європи з підвищення безпеки людини в кіберпросторі та загальноєвропейському правовому просторі. Проте процес модернізації зазначеної Конвенції, в якому Україна бере активну участь, ще триває, враховуючи динамічний розвиток та випуск підзаконних та інших нормативно-правових актів[59].

Політика Китаю у сфері кібербезпеки заслуговує особливого уваги та критики. Починаючи з 2000 року, Китай створив спеціальні підрозділи кіберполіції для збереження порядку в інтернет-просторі. Особливу увагу приділяють вдосконаленню засобів контролю за мережею та розробці «кібервійської» стратегії. Одночасно, виникає важливе питання про використання так званої «мудрої сили», що передбачає поліпшення іміджу держави.

Варто згадати американський Закон «Про інформаційну безпеку» 1987 року. Основною метою цього закону є забезпечення мінімально необхідних заходів для безпеки інформації у федеральних комп'ютерних системах, без обмежень всього спектру можливих дій. Відповідно до цього закону, всі оператори федеральних інформаційних систем, що містять конфіденційну інформацію, зобов'язані розробити плани забезпечення інформаційної безпеки. Також усі урядові відомства мають сформувати плани забезпечення інформаційної безпеки, спрямовані на компенсацію ризиків і запобігання

[59] Почепцов Г. Г. Інформаційна політика та інформаційні війни: навч.- метод. посіб. Київ: Вид-во НАДУ, 2012. С. 85-86.

можливим збиткам від втрати, неправильного використання, несанкціонованого доступу або модифікації інформації у федеральних системах[60].

У сучасному світі інформаційна безпека стає однією з найбільш важливих складових для всіх країн, що входять до Європейського Союзу. Захист персональних даних, визначений Директивою 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних», є невід'ємною частиною цього процесу[61].

У Польщі правовою основою інформаційної політики слугують різноманітні закони, такі як «Закон про пошту і телекомунікації», «Закон про телебачення і радіомовлення», «Закон про державні відносини з римською католицькою церквою в Республіці Польща». Ці закони визначають напрями інформаційної політики, встановлюють технологічні стандарти інформаційного зв'язку та регулюють права церкви на інформаційну діяльність[62].

У Польщі також діє неурядова організація, Центр аналізу пропаганди і дезінформації, яка спрямовує зусилля на аналіз та протидію російській дезінформації в польському інформаційному просторі. Захоплюючим ідеям та досвіду Польщі можна навчитися, особливо у зв'язку з інформаційними загрозами з боку Росії, що є актуальним і для України[63].

У Румунії відбувається активна розбудова системи кібернетичної безпеки, у якій ключову роль відіграє Румунська служба інформації. Важливою є ініціатива Молдови, що здійснюється через Національну стратегію розвитку інформаційного суспільства «Moldova digitală 2020», яка враховує проблеми безпеки кіберпростору[64].

---

[60] Сливка М.М., Лук'янова Г.Ю. Правове забезпечення інформаційної безпеки: досвід країн Європейського Союзу // Юридичний науковий електронний журнал. 2021. № 11. С. 514.

[61] Там само. С. 515.

[62] Тихомирова Є.Б., Смик Р.П. Інформаційна політика Польщі // Сучасні проблеми гуманітаристики: світоглядні пошуки, комунікативні та педагогічні стратегії: матеріали V Всеукраїнської науково-практичної конференції. Рівне, 2015. С. 113.

[63] Там само. С. 113-114.

[64] Климчук О.О., Ткачук Н.А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки // Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С. 79.

Ці приклади інформаційних стратегій в регіоні можуть стати джерелом навчання та вдосконалення для інших країн, включаючи Україну, в контексті сучасних викликів у сфері безпеки та інформаційних технологій.

Отже, зарубіжний досвід однозначно демонструє, що державні структури відіграють невід'ємну та вирішальну роль у координації заходів, спрямованих на забезпечення інформаційної безпеки. Важливою складовою цього процесу є постійне удосконалення законодавства, яке встановлює правила та відповідальність за порушення закону в цій сфері.

Напрямком розвитку є розробка та прийняття законів, що чітко визначають правопорушення та типи відповідальності за них в контексті інформаційної безпеки. Це означає не лише удосконалення існуючого законодавства, але й створення нових нормативно-правових актів, які враховуватимуть сучасні виклики та загрози у сфері інформаційної безпеки.

Прийняття таких законів сприятиме створенню прозорого та ефективного правового середовища, яке забезпечить ефективний контроль за дотриманням правил і норм безпеки, а також відповідальність за їх порушення. Такий підхід допоможе покращити рівень захисту інформації та забезпечити безпеку суспільства в цифрову епоху.

РОЗДІЛ ІІІ. НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Забезпечення інформаційної безпеки України та захисту національних інтересів в цій сфері на сучасному етапі передбачає пріоритетний розвиток системи нормативно-правового регулювання відносин у цій сфері, а також протидію загрозам цих інтересів та упорядкування правотворчого процесу.

Спочатку, в умовах розбудови правової держави та громадянського суспільства діяльність органів державної влади, які несуть основну відповідальність за національну безпеку, має бути регульована конкретними правовими нормами. Ці норми гарантують конституційні права та свободи громадян. Правові акти у цій сфері спрямовані на закріплення цілей протидії загрозам національної безпеки України, засобів та методів їх досягнення, а також на забезпечення узгодженої політики органів влади.

По-друге, інтеграція України в міжнародне співтовариство розширює можливості забезпечення інформаційної безпеки держави через участь у розвитку норм міжнародного права та створення міжнародних механізмів забезпечення безпеки інформаційної сфери.

По-третє, гарантування прав та свобод громадян і захист національних інтересів передбачає активну участь держави в регулюванні відповідних суспільних відносин та наявність прозорої державної політики в цій сфері.

Останнім часом органи державної влади та науковці приділяють значну увагу обговоренню проблем удосконалення правового забезпечення інформаційної безпеки України. Це правове забезпечення формується системою правового регулювання, що включає в себе масив правових норм, які регулюють відносини в цій сфері, а також акти, що виникають на їх основі та право-засновчі документи.

Правові норми є основою забезпечення інформаційної безпеки та визначають ефективність діяльності держави, суспільства та окремих громадян у захисті національних інтересів України в інформаційній сфері. У цю базу

включаються норми міжнародних договорів, законодавчі акти України, акти Президента України, урядові постанови, а також нормативні акти органів державної влади, які регулюють відносини у цій сфері.

Необхідність правового забезпечення демократичних перетворень у суспільстві та державі передбачає реформування всієї правової системи України, зокрема її законодавства, оскільки існуюче законодавство має суттєві недоліки. У зв'язку з цим Україні довелося приймати ряд нормативно-правових актів, що відповідають європейським стандартам.

Аналіз стану правового регулювання інформаційної безпеки України проводиться з урахуванням трьох структурних елементів інформаційної безпеки: у сфері прав і свобод людини та громадянина, інформаційно-психологічної безпеки та інформаційно-технічної безпеки[65].

Враховуючи широкий спектр нормативно-правових актів, які регулюють взаємини у сфері інформаційної безпеки України, вважаємо за важливе проаналізувати концептуальні аспекти цього питання.

Сучасна стратегія адміністративно-правового забезпечення інформаційної безпеки України включає аналіз та удосконалення нормативно-правового регулювання в цій сфері. Особливу увагу приділяється регулюванню інформаційної безпеки у сфері прав і свобод. Для цього використовуються Конституція України та базові закони держави, такі як «Про інформацію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», та інші. Ці акти регулюють питання забезпечення інформаційної безпеки, захисту інформації, охорони державної таємниці та забезпечення конфіденційності інформації.

Проте, існує ряд проблем у цій сфері. Однією з них є розпорошення нормативно-правового регулювання в різних актах різної юридичної сили, а також недолік узгодженості цих актів між собою та з Конституцією. Багато норм є декларативними і не містять конкретних шляхів їх реалізації, що призводить до

[65] Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: Дис. … канд. юрид. наук. Київ, 2007. С. 117.

низького рівня реалізації правових норм, які регулюють суспільні відносини в сфері інформаційної безпеки.

Аналіз нормативно-правових актів в сфері інформаційної безпеки України підкреслює необхідність удосконалення законодавства. Інформаційна безпека України є невід'ємною частиною національної безпеки і важливою складовою для формування базових знань та уявлень про загальну безпеку. Розвиток інформаційного законодавства спрямований на забезпечення гарантованого рівня національної безпеки в інформаційній сфері та нормального функціонування інформаційних технологій і засобів захисту[66].

Проблема забезпечення національних інтересів і безпеки в інформаційній сфері залишається на етапі активної розробки. Для забезпечення інформаційної безпеки використовується єдина державна політика, яка базується на системі заходів економічного, політичного і організаційного характеру, що адаптовані до загроз і небезпек, що ставлять під загрозу національні інтереси особи, суспільства і держави в інформаційній сфері.

Створення та підтримання належного рівня інформаційної безпеки вимагає розробки системи правових норм, регулювання відносин в інформаційній сфері, визначення основних напрямів діяльності державних органів, формування або перетворення органів та механізмів контролю і нагляду.

Важливо враховати висловлення В.А. Ліпкана, який зазначає, що система забезпечення інформаційної безпеки не обмежується лише наявністю великого обсягу нормативно-правових актів. [67]. Це свідчить про несформованість системи забезпечення національної безпеки, невизначеність національної та інформаційної політики і недосконаліть нормативно-правового регулювання в цій сфері.

Законодавча база України у сфері інформаційної безпеки є неповною і потребує вдосконалення. Наприклад, 11 січня 2011 року Верховна Рада України прийняла за основу проєкт Закону України «Про Концепцію державної

[66] Ліпкан В.А. Національна безпека України: Навч. посіб. 2-ге вид. Київ, 2009. 576 с.
[67] Ліпкан В.А. Національна безпека України: Навч. посіб. 2-ге вид. Київ, 2009. 576 с.

інформаційної політики України», який визначає мету, принципи, пріоритетні завдання та основні напрямки діяльності держави у цій сфері. Концептуальні основи державної політики інформаційної безпеки та сфери обігу інформації розробляються з урахуванням вихідних положень функціонального підходу до управління.

Інтеграція України у світовий інформаційний простір, створення єдиної системи охорони та технічного захисту обмеженої доступності інформації, а також забезпечення безпеки інформаційно-телекомунікаційних систем та мереж зв'язку, включаючи Інтернет, є ключовими завданнями. Важливо також захищати національні інтереси у міжнародному співробітництві та прогнозувати ризики у політичній, економічній, соціальній та інших сферах.

Необхідно адекватно реагувати на негативні фактори інформаційної безпеки, а також брати участь у міжнародних системах безпеки. Забезпечення керівництва, координації та контролю в цій сфері також є важливим аспектом.

Недостатнє правове регулювання у цій сфері ускладнює налагодження суспільних відносин. Щоб ефективно боротися з цим, необхідно розробити науково обгрунтовану державну інформаційну політику.

Згідно зі звітом Всесвітнього економічного форуму про розвиток інформаційних технологій, Україна виявляється на 43-му місці серед 139 країн у рейтингу розвитку інформаційно-комунікаційних технологій у 2018 році (у 2016 році – на 64-му місці).

Ця статистика підкреслює потребу в постійному вдосконаленні законодавства, формуванні внутрішньо узгодженої нормативно-правової бази та створенні умов для одночасної трансформації елементів державно-правової структури. Особливу увагу слід звернути на нові характеристики інформаційно-комунікаційних технологій, які потрібно враховувати при розробці та впровадженні відповідної правової політики[68].

[68] Богуш В.М. Інформаційна безпека держави. Київ: МК-Прес, 2005. 431 с.

Негативні аспекти у розвитку системи національного законодавства та її адаптації до вимог Європейського Союзу можуть порушувати цей процес.

Розвиток правового регулювання використання інформаційних технологій характеризується спробами вирішити протиріччя і встановити гармонійну правову систему, але швидкий розвиток технологій часто спричиняє нові протиріччя. Необхідний баланс в системі правових норм, що регулюють інформаційні відносини, не завжди досягається, оскільки правові засоби обмежені суспільним розвитком.

Процес законотворчості ускладнено відсутністю чіткої системи регулювання правових відносин і стрімким розвитком цього сегменту законодавства. За період діяльності Комітету з питань цифрової трансформації інформатизації Верховної Ради України протягом трьох сесій дев'ятого скликання було розглянуто 35 законопроєктів (станом на 26 червня 2020 року). Це свідчить про важливість поєднання правотворчої роботи з систематизацією законодавства.

Наукове дослідження щодо розвитку інформаційного законодавства за 2020 рік провели такі вчені, як І. Арістов, О. Баранов, В. Бєлєвцев, Д. Біленський, Н. Бортник, В. Брижко, В. Ліпкан та інші. Вони запропонували поділити інформаційні відносини на два блоки: перший - це питання, пов'язані безпосередньо з інформацією, технологіями та системами зв'язку; другий - це питання, які становлять об'єкт регулювання в інших сферах, але мають велике значення для розвитку законодавства в сфері інформації, технологій та інформаційної безпеки. Поточні закони в цій області створюють різноманітні інформаційно-правові режими, включаючи правове регулювання інформаційної безпеки.

Однак, часто закони в інформаційній сфері приймаються без системного підходу і не вирішують певних проблем (наприклад, проєкт закону «Про хмарні послуги», де не враховують питання інформаційної безпеки).

У деяких випадках встановлення цілей у законодавстві не враховує наявних засобів інформаційних технологій, що може призвести до

неоптимального використання ресурсів, а також до потреби внесення змін у нормативні акти. У інших, навпаки, встановлені цілі можуть бути визначені без урахування наявних засобів, що ускладнює їх реалізацію. Це зазвичай призводить до невизначеності у питаннях регулювання інформаційних відносин.

Законодавство у сфері інформаційних технологій часто змінюється шляхом внесення змін до діючих законів, що ускладнює створення систематичного підходу до цієї галузі. Для вирішення цих проблем необхідно послідовно впроваджувати принципи, такі як правова визначеність та пропорційність, щоб забезпечити інформаційну безпеку та уникнути соціально-правових конфліктів. Так як будь-який недолік у нормативно-правовому регулюванні інформаційної безпеки, так і в інших сферах, намагаються вирішити або принаймні зменшити його масштаби. Проте зробити це складно через різноманітні обставини. Однією з головних причин законодавчого дисбалансу в цій сфері є невідповідність системи нормативно-правових актів і норм їхньому історичному контексту та розвитку суспільства[69].

З цієї точки зору, недосконаліть інформаційного законодавства є практично непомітною, оскільки суспільне життя завжди містить ряд суперечностей, а законодавство намагається створити систему, яка б ураховувала ці суперечності. Проблема ускладнюється постійною зміною суспільних відносин, що відбувається в контексті розвитку інформаційного суспільства. Щоб зробити правову систему більш адаптивною до цих змін, необхідно проводити комплексне удосконалення, враховуючи різні аспекти загальної теорії права.

Удосконалення законодавства в цій сфері може відбуватися на двох рівнях: шляхом зміни нормативних актів на рівні законів або за допомогою підзаконних нормативних актів. Обидва підходи мають свої переваги і недоліки, і важливо забезпечити баланс між ними.

[69] Писаренко Т. В., Кваша Т. К. Стан інноваційної діяльності та діяльності у сфері трансферу технологій в Україні у 2018 році: аналітична довідка. Київ: УкрІНТЕІ, 2019. 80 с.

Формування правових засад інформаційної безпеки пов'язане з міжнародним досвідом і повинно базуватися на принципах системності та збалансованості з урахуванням міжнародних стандартів і норм. З розвитком нових інформаційних технологій в Інтернеті гуманітарні і економічні відносини проходять значні зміни, що породжує потребу в регулюванні цього простору. Проте таке регулювання не може бути обмеженим лише національними рамками і потребує урахування міжнародних аспектів.

Наявність «часткового» законодавства в сфері інформаційного права може пояснюватися особливостями його предмету, який включає у себе регулювання інформаційних відносин та умови поведінки суб'єктів права у цій сфері.

Розширюючи концепцію О. Баранова про дві складові інформаційного законодавства, можна виділити дві основні частини. По-перше, це власне інформаційне законодавство, яке охоплює предмет та інститути інформаційного права у повному обсязі. По-друге, це міжгалузевий інформаційний «блок», який є складовою частиною законодавства у кожній галузі.

Інформаційне законодавство виступає як сполучна ланка у системі законодавства, спрямована на уніфікацію та єдність регулювання інформаційних процесів у всіх сферах життя. Треба відзначити, що міжгалузевий блок за обсягом переважає саме інформаційне законодавство.

Систему правового регулювання інформаційної безпеки можна поділити на дві частини: загальну і особливу. У загальній частині встановлюються основні поняття, принципи, термінологія, методи та механізми регулювання суспільних відносин, пов'язаних з захистом інформації та інформаційної інфраструктури. Особлива частина включає окремі інститути, які регулюють окремі інформаційні технології, наприклад, хмарні послуги.

Відповідно до Е. Шмідта та Д. Коена, закон Мура стверджує, що чіпи процесорів стають вдвічі швидшими кожні вісімнадцять місяців, а кількість даних, що передається оптоволоконними кабелями, подвоюється кожні дев'ять місяців. Це підтверджує динамічний характер систематизації законодавства у

сфері інформаційної безпеки, який обумовлений рівнем розвитку суспільства та динамікою технологій[70].

Інформаційна сфера має значну кількість нормативних актів, але сам предмет регулювання інформаційної безпеки стрімко змінюється, що часто перевершує темпи законодавчого та підзаконного регулювання. М. Кайку зазначає, що найбільші зміни можуть відбутися у сфері експертних систем, де закодована людська мудрість і досвід.

Швидкі зміни в інформаційних технологіях та розвиток Інтернету постійно впливають на традиційні галузі права, змінюючи їхні норми та інститути, такі як електронна комерція та електронні документи. З цієї точки зору, вважається доцільним вносити зміни в окремі закони на даному етапі, ніж створювати кодекс, який може застаріти через швидкі технологічні зміни.

В теперішній час деякі недоліки, пов'язані з відсутністю нормативного регулювання інформаційної безпеки, компенсуються великою кількістю корпоративних нормативно-правових положень. Однак з огляду на реформування державного управління стає набагато актуальнішим питання систематизації адміністративного законодавства та його впливу на інформаційну безпеку. Це охоплює не лише відносини з організацією діяльності суб'єктів інформаційних відносин, але й стосунки з громадянами та громадянським суспільством, які виникають в цьому контексті.

Окремо варто зазначити питання адміністративно-правових заходів для захисту особистих прав громадян у сфері інформаційної безпеки в різних сферах життєдіяльності, які регулюються адміністративним та інформаційним законодавством і потребують відповідного контролю та нагляду державних органів.

Незважаючи на те, що виконання стратегічних актів передбачає застосування методів соціально-економічного прогнозування та планування, це

[70] Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 р. № 1678-VII.

стає передумовою для подальшого розвитку прогнозування у законодавстві. Більшість економічних прогнозів включають розробку прогнозів розвитку законодавства. Обрання певного напряму соціально-економічного розвитку держави, зокрема асоціація з Європейським Союзом та НАТО, передбачає адаптацію національного законодавства та вимагає його коригування та оновлення з урахуванням поставлених цілей та завдань.

Розвиток законодавства - складний процес, який залежить від безлічі різноманітних факторів. Недостатнє наукове передбачення, поспішність у підготовці актів, помилки в розрахунках, недостатність аналітичної інформації та недоліки у врахуванні соціальних факторів можуть погіршити якість правових актів.

Як було вказано раніше, діюче національне законодавство у сфері інформаційної безпеки характеризується недостатньою системністю, суперечливістю та наявністю прогалин.

Варто відзначити, що перелік законодавчих актів у галузі інформаційної безпеки є достатньо широким. Однак при розробці законів, спрямованих на регулювання специфічних відносин, відповідні можливості частково не використовуються. Існування значної кількості правових норм ускладнює ситуацію, коли порушення законів не завжди призводить до юридичної відповідальності, а відсутність чітких механізмів забезпечення доступу до відкритої інформації державних органів може обмежити права і свободи людини та громадянина[71].

Однією з основних правових проблем, що виникають у зв'язку з еволюцією інформаційних технологій у сфері електронних комунікацій, є поява нових учасників правових процесів, які беруть активну участь у процесі універсального обслуговування та користування інформаційною індустрією.

Важливо розглядати відкриті інформаційні системи у контексті глобальної концепції розвитку інформаційних технологій, що сприяє розповсюдженню

[71] Баранов О. А. Напрями перспективних досліджень у галузі інформаційного права // Інформація і право. 2016. № 2 (17). С. 15–31.

інформаційного продукту і розмиттю меж між змістом інформації та засобом її передачі. У таких умовах склад і особливості правового статусу учасників відносин у сфері захисту інформації в мережах електронних комунікацій змінюються значно, що потребує нових підходів до правового регулювання забезпечення інформаційної безпеки.

Однак з огляду на невизначеність механізмів та часті помилки при прийнятті нормативних актів і управлінських рішень, а також можливі негативні соціальні наслідки, актуальним є дослідження потенціалу прогнозування динаміки інформаційного законодавства, зокрема у сфері забезпечення інформаційної безпеки, як засобу попередження можливих проблем. [72]

Отже, розвиток правової науки та вирішення актуальних завдань забезпечення інформаційної безпеки вимагають уваги до технологій прогнозування законодавства в інформаційній сфері.

Я акцентую увагу на теоретичних засадах методології, оскільки головне завдання з реалізації прийнятих законів покладено на державні органи.

У контексті математичної моделі правового прогнозування, у поєднанні з методологією порівняльного правознавства стосовно інформаційного законодавства країн ЄС, розвиток національного інформаційного законодавства у сфері інформаційної безпеки передбачає збільшення частки відомчих і корпоративних нормативно-правових актів. Ці акти будуть доповнювати основні інформаційні закони та вносити зміни у чинні нормативно-правові акти інформаційно-комунікаційної складової, яка регулює інформаційні відносини у певних галузях суспільних відносин.

Світовий досвід в котре підтверджує, що ефективне регулювання відносин в інформаційній сфері сприяє стимулюванню творчого процесу у всіх сферах життєдіяльності людини.

[72]Шмідт Е., Коен Д. Новий цифровий світ; пер. з англ. Г. Лелів. Львів: Дітопис, 2015. 304 с.

РОЗДІЛ IV. СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЇ. АДАПТАЦІЯ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА ДО ЄВРОПЕЙСЬКОГО

Після розпаду Радянського Союзу на міжнародній арені з'явилися нові незалежні країни, включаючи Україну. Відразу ж після оголошення незалежності 2 грудня 1991 року, Європейський Союз випустив Декларацію про Україну, визнаючи тим самим її суверенітет.

Крім того, Директива Європейського Співтовариства щодо визнання нових держав у Східній Європі та колишньому Радянському Союзі від 16 грудня 1991 року, заявила про готовність ЄС та його держав-членів визнати нові держави, які створилися на демократичних засадах, прийняли міжнародні зобов'язання та прагнуть до миру і переговорів.

Угода про торгівлю та співробітництво між Радянським Союзом і Європейським Співтовариством, укладена 18 грудня 1989 року, була замінена Угодою про партнерство і співробітництво (УПС), укладеною між новою незалежною Україною та Європейськими Співтовариствами та їх державами-членами. Ця Угода була підписана 14 червня 1994 року та ратифікована Законом України 10 листопада 1994 року. Зараз майже з усіма державами, що виникли внаслідок розпаду СРСР, укладено аналогічні Угоди. В Основних напрямах зовнішньої політики України, схвалених Верховною Радою 2 липня 1993 року, зазначено, що укладання Угоди про партнерство та співробітництво з Європейськими Співтовариствами є першим кроком до асоціації та, в подальшому, до повного членства в цій організації [73].

Стаття 51 Угоди передбачає, що сторони визнають зближення законодавства України з законодавством Європейського Союзу як важливу умову для підтримки зв'язків між Україною та ЄС. Україна зобов'язується приводити своє законодавство у відповідність з законодавством ЄС.

[73] Європейський вибір. Концептуальні засади стратегії еко номічного та соціального розвитку України на 2002-2011 роки: Послання Президента України до Верховної Ради // Урядовий кур'єр. 2002. 4 червня.

Також важливою є норма, згідно з якою Європейське Співтовариство зобов'язується надавати Україні належну технічну допомогу для здійснення вищезазначених заходів, включаючи обмін експертами, надання інформації та організацію семінарів.

Укладення Угоди між Україною та Європейським Співтовариством про наукове і технологічне співробітництво 4 липня 2002 року було логічним наступом після Угоди про партнерство і співробітництво (УПС), яка стала частиною внутрішнього законодавства України у 1994 році. Ця нова угода визначила основні напрямки співробітництва, серед яких важливе місце займають технології інформаційного суспільства та науково-технологічна політика.

Окрім цього, угода передбачила створення спеціального інституційного механізму - Ради Співробітництва. Ця Рада складається з представників Ради Європейського Союзу, Комісії ЄС та урядів нових незалежних держав. Крім того, було створено Комітет з питань співробітництва та Комітет з парламентського співробітництва, які забезпечують ефективний діалог та співпрацю[74].

Щодо імплементації положень УПС, нові незалежні держави можуть вживати різноманітних заходів, зокрема, укладати двосторонні договори, приймати внутрішні нормативні акти відповідно до acquis або приєднуватися до багатосторонніх договорів.

Важливо також підкреслити, що Україна визначила стратегію інтеграції до Європейського Союзу ще в 1998 році, у якій закликається до чіткого та всебічного визначення зовнішньополітичної стратегії щодо інтеграції України до європейського політичного, інформаційного, економічного та правового простору.

На основі Стратегії інтеграції України до Європейського Союзу, яка була затверджена 14 вересня 2000 року, було прийнято ряд важливих документів,

[74] Про Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу Закон України від 18 березня 2004 року.

включаючи Програму інтеграції, Концепцію Загальнодержавної програми адаптації законодавства України до ЄС, та Загальнодержавну програму адаптації законодавства України до законодавства ЄС. Для координації цих процесів було створено Національну раду з питань адаптації законодавства України до законодавства ЄС, а також введено єдину систему планування, координації та контролю роботи з адаптації законодавства за Указом Президента України.

Важливо відзначити, що активність у сфері інтеграції притаманна і Європейському Союзу, що виявляється через ряд стратегічних документів, серед яких вирізняється Спільна стратегія ЄС щодо України від 11 грудня 1999 року.

На саміті ЄС - Україна у Копенгагені 4 липня 2002 року була підтверджена готовність продовжувати співробітництво у пріоритетних сферах та надавати імпульс зближенню, що сприяє створенню внутрішніх передумов для майбутнього набуття Україною членства в Європейському Союзі. Бажання України приєднатися до Європейського Союзу вимагало обов'язкового прийняття «acquis communautaire» - сукупності цілей, принципів, норм спільної політики та законодавства ЄС, а також юридичних та інституційних механізмів їхнього впровадження. На момент його виникнення «acquis communautaire» включав такі елементи як:

1) основоположні міжнародні договори, які закладали основи Європейських Співтовариств;

2) інституційну структуру Співтовариств;

3) законодавство Співтовариств;

4) міжнародні договори, укладені Співтовариствами;

5) акти, прийняті країнами-кандидатами у процесі приєднання до ЄС;

6) довгострокові цілі, які перебувають у процесі визначення;

7) обов'язок нового члена визнати такі основоположні принципи права Європейських Співтовариств, як пряма дія, примат права Співтовариств над національним правом їх членів, та однакове тлумачення права Співтовариств всіма їх членами.

Стандарти ЄС вважалися еталоном, хоча, як показує історія, були випадки, коли вони не відповідали, а навіть були нижчими за стандарти країн, що подавали заявки на членство. Наприклад, високі екологічні стандарти деяких країн-членів. Це спонукало ЄС до цілеспрямованих заходів щодо підвищення стандартів членів ЄС до рівня країн, що мали подати заявки на вступ.

Ця активність призвела до різноманітних проблем у процесі впровадження «acquis». Наприклад, складність структури «acquis», включаючи неузгодженість в фундаментальних поняттях, існування застарілих норм, та потребу реформування національного законодавства для визнання примату європейського права та верховенства Європейського Суду. Також важливою є нестабільність деяких галузей «acquis» та потреба внутрішньої реформи самого ЄС, щоб забезпечити ефективне виконання стандартів.

У Посланні Президента України до Верховної Ради України «Європейський вибір: Концептуальні засади стратегії економічного та соціального розвитку України на 2002-2011 роки» планувалося на період 2002-2007 років приведення законодавства України у відповідність до вимог законодавства ЄС у пріоритетних сферах. З метою забезпечення цієї адаптації був створений Державний департамент адаптації законодавства, який має наступні завдання:

1. Організація виконання державної політики у сфері адаптації законодавства України до законодавства ЄС.
2. Участь у координації виконання Загальнодержавної програми адаптації законодавства України до законодавства ЄС.
3. Забезпечення науково-експертного та інформаційного забезпечення євроінтеграції.
4. Розроблення рекомендацій щодо приведення законодавства України у відповідність з «acquis communautaire» та розроблення проектів нормативно-правових актів на цій основі.
5. Експертиза проектів законів та інших нормативно-правових актів на відповідність «acquis communautaire».

6. Зведення інформації про стан адаптації законодавства України до законодавства ЄС.

7. Організація моніторингу імплементації актів законодавства України, які розроблені відповідно до «acquis communautaire».

8. Координація співробітництва між Україною та ЄС у сфері адаптації законодавства України до законодавства ЄС та у сфері юстиції і внутрішніх справ[75].

Однією з важливих функцій Департаменту є організація перекладу актів «acquis communautaire» на українську мову та надання їм офіційного статусу. Цей процес здійснюється на основі щорічного плану, який розробляється Департаментом за участю центральних органів виконавчої влади та структурних підрозділів Департаменту.

Механізм цього процесу регулювався наказом № 56/5 Міністерства юстиції України «Про затвердження Порядку перекладу актів acquis communautaire на українську мову» від 08.06.2005 року (у 2009 році – втратив чинність)[76].

Отож, важливо зауважити, що навіть якщо будь-яка з колишніх радянських республік, розташована в Європі, відповідає усім критеріям для вступу до ЄС і не має жодних об'єктивних причин для відмови, інтеграційний процес все одно залишатиметься політичним, і критерії для вступу можуть бути свідомо формальними.

Необхідно розуміти, що багато хто не бажає бачити Україну в Європейському Союзі. Щоб Україна могла приєднатися до ЄС, вона повинна мати розвинене інформаційне суспільство, процвітаючу економіку та ефективну систему безпеки. В іншому випадку, постійне прагнення відповідати критеріям може перетворити функціонування України на безперервну боротьбу за

[75] Угода про партнерство та співробітництво між Україною і Європейськими співтовариствами та їх державами-членами, підписана 14 червня 1994 р. в Люксембурзі, ратифікована Законом України від 10 листопада 1994 року.

[76] Наказ Про затвердження Порядку перекладу актів acquis communautaire на українську мову за N 642/10922 від 08.06.2005 р.

відповідність, а нові критерії можуть з'являтися після досягнення попередніх цілей. Замість цього, Україні слід використовувати найкращі практики законодавства та його застосування для будівництва процвітаючого демократичного суспільства і могутньої держави.

Тому важливо, щоб українська сторона активно співпрацювала з Євросоюзом для формування ефективного механізму реалізації національних інтересів. Адаптація має стосуватися не тільки українського законодавства, але й стандартів Європи, щоб створити підвалини для стійкого розвитку України. Наша мета - не лише пристосуватися до стандартів, але й використовувати їх для побудови кращого майбутнього.

В контексті проблематики розділу варто відзначити, що Угоду про партнерство та співробітництво замінила в 2014 році *Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони*. Політичну частину угоди було підписано 21 березня 2014 року, економічну частину — 27 червня 2014 року.

ВИСНОВКИ

Отже, інформаційна безпека є ключовим аспектом функціонування сучасного суспільства, оскільки вона включає у себе інтереси особистості, суспільства та держави. Забезпечення інформаційної безпеки передбачає не лише захист від зовнішніх загроз, але й забезпечення якості інформаційних систем для всіх суб'єктів.

Держава відіграє важливу роль у визначенні відповідних органів та механізмів регулювання та контролю інформаційних процесів. Особливу увагу потрібно приділити залежності української інформаційної інфраструктури від зарубіжних технологій і захисту національних інтересів у цій сфері.

У результаті дослідження правового забезпечення інформаційної безпеки України можна зробити кілька важливих висновків.

По-перше, сучасне українське законодавство у сфері інформаційної безпеки охоплює широкий спектр питань, починаючи від конституційних норм до спеціальних законів, що регулюють цю сферу. Проте, необхідно постійно оновлювати та адаптувати законодавство до змін у суспільстві та технологічному прогресі.

По-друге, забезпечення інформаційної безпеки вимагає системного підходу, що охоплює як технічні аспекти захисту інформації, так і правові та організаційні заходи.

По-третє, успішна реалізація політики інформаційної безпеки потребує активної співпраці з міжнародними партнерами та адаптації до міжнародних стандартів у цій сфері. Широке ознайомлення громадськості з важливістю заходів забезпечення інформаційної безпеки, спільна робота різних галузей та постійне оновлення концептуальних документів є ключовими компонентами успішної реалізації цієї політики.

По-четверте, важливо забезпечити широке ознайомлення громадськості з важливістю заходів забезпечення інформаційної безпеки, а також залучення різних галузей та органів влади до спільної роботи у цьому напрямку.

Правове забезпечення інформаційної безпеки включає широкий спектр заходів та інструментів, які регулюють відносини у сфері інформаційної діяльності. Українське законодавство у цій сфері охоплює норми різних правових галузей і стрімко розвивається відповідно до європейських стандартів.

У цифрову епоху важливо створити безпечне та стійке інформаційне середовище, яке сприятиме розвитку інформаційного суспільства та забезпечить захист прав індивідуумів та інтересів суспільства. Такий комплексний підхід вимагає проведення технічних, організаційних, політичних та міжнародно-правових заходів.

Узагальнюючи, правове забезпечення інформаційної безпеки України є складною та багатогранною проблемою, яка вимагає постійного вдосконалення та узгодженого підходу від усіх суб'єктів. Це доволі важливий аспект для забезпечення стабільності та розвитку нації в умовах сучасного інформаційного суспільства та війни українського народу із агресором - Російською Федерацією, яка використовує інформаційні ресурси як методи пропаганди та дискримінації української нації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

I. Джерела

1. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003. URL: https://zakon.rada.gov.ua/laws/show/995_c57#Text (дата звернення: 07.02.2024).
2. Європейський вибір. Концептуальні засади стратегії економічного та соціального розвитку України на 2002-2011 роки: Послання Президента України до Верховної Ради // Урядовий кур'єр. 4 червня. 2002. URL: https://zakon.rada.gov.ua/laws/show/n0001100-02#Text (дата звернення: 07.02.2024).
3. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. Неофіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 07.02.2024).
4. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р. № 851-IV // Відомості Верховної Ради України. URL: http://zakon.rada.gov.ua/go/851-15 (дата звернення: 07.02.2024).
5. Законопроєкти опрацьовані Комітетом протягом роботи третьої сесії Верховної Ради України IX скликання // Офіційний портал Верховної Ради України. URL: https://komit.rada.gov.ua/news/zp_na_roz/73474.html (дата звернення: 07.02.2024).
6. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: ратифікація від 06.07.2010l, N 2438-VI. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 07.02.2024).
7. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР: із змінами та доповненнями від 01.01.2020 р. № 27-IX // Відомості Верховної Ради України. URL: https://www.president.gov.ua/documents/constitution (дата звернення: 07.02.2024).

8. Концепція (основи державної політики) національної безпеки України: схвалено постановою Верховної Ради України від 16.01.1997 // Урядовий кур'єр. 1997. URL: https://zakon.rada.gov.ua/laws/show/3/97-%D0%B2%D1%80#Text (дата звернення: 07.02.2024).

9. Митний кодекс України: із змінами і доповненнями, внесеними Законами України від 13 квітня 2012 року, N 4652-VI. URL: https://ips.ligazakon.net/document/T020092?an=688154 (дата звернення: 07.02.2024).

10. Наказ Про затвердження Порядку перекладу актів acquis communautaire на українську мову за N 642/10922 від 08.06.2005 р. // Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/z0642-05#Text (дата звернення: 08.02.2024).

11. Податковий кодекс України: Кодекс від 02.12.2010 р. № 2755-VI // Відомості Верховної Ради України. URL: http://zakon2.rada.gov.ua/laws/main/2755-17 (дата звернення: 07.02.2024).

12. Податковий кодекс України: редакція від 01.01.2024 року. URL: https://buhgalter911.com/uk/normativnaya-baza/nalogovyi-kodeks/ (дата звернення: 07.02.2024).

13. Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Постанова Кабінету Міністрів України від 25.10.2017 р. № 1106. URL: https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF#Text (дата звернення: 07.02.2024).

14. Про Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу Закон України від 18.03.2004 р., № 1629-IV // Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1629-15#Text (дата звернення: 07.02.2024).

15. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.94, № 81/94-ВР: із змінами, внесеними від 16.12.2020, № 1089-IX // Відомості Верховної Ради України. URL:

https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 07.02.2024).

16. Про національну безпеку України: Закон України // Відомості Верховної Ради, № 31, ст. 241, 2018. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 07.02.2024).

17. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V // Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 07.02.2024).

18. Про прийняття за основу проєкту Закону України «Про Концепцію державної інформаційної політики»: Постанова Верховної Ради України від 11.01.2011 № 2897-VI. // Відомості Верховної Ради України. URL: http://zakon1.rada.gov.ua (дата звернення: 07.02.2024).

19. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 р. № 1678-VII // Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1678-18#Text (дата звернення: 07.02.2024).

20. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020 // Відомості Верховної Ради України. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 07.02.2024).

21. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Презедента України від 13.02.2017 №47 // Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/32/2017#Text (дата звернення: 07.02.2024).

22. Про хмарні послуги: Проект Закону України від 20.12.2019 р. № 2655 // Відомості Верховної Ради України. URL:

http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67744 (дата звернення: 07.02.2024).

23. Угода про партнерство та співробітництво між Україною і Європейськими співтовариствами та їх державами-членами, підписана 14 червня 1994 р. в Люксембурзі, ратифікована Законом України від 10 листопада 1994 року // Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/998_012#Text (дата звернення: 07.02.2024).

24. Building the Information Society: Moving Canada into the 21st Century / Ministry of Supply and Services. Ottawa, 1996. 64 p.

25. Information Superhighway: An Overview of Technology Challenges / USA Congress. Washington, 1995. URL: https://www.gao.gov/products/aimd-95-23 (дата звернення: 07.02.2024).

II. Література

1. Алямкін Р. В. Правове забезпечення національної інформаційної безпеки // Наукові записки Інституту законодавства Верховної Ради України. 2013. № 4. С. 91-96.

2. Андріюк В. В. Теоретико-методологічні основи юридичного прогнозування: дис. ... канд. юрид. наук: 12.00.01 / Прикарпатський національний ун-т ім. Василя Стефаника. Івано-Франківськ, 2006. 207 с.

3. Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні // Підприємництво, господарство і право. 2019. № 9. С. 100-108.

4. Баранов О. А. Напрями перспективних досліджень у галузі інформаційного права // Інформація і право. 2016. № 2 (17). С. 15–31.

5. Бєляков К. І. Деякі питання щодо формування реформи інформаційного законодавства України // Систематизація законодавства в Україні: проблеми теорії і практики: матеріали міжнародної науково-практичної конференції. Київ: Інститут законодавства Верховної Ради України, 1999. С. 253-255.

6. Бліхар М. М. Адміністративно-правове забезпечення інформаційної безпеки в інтернет просторі // Науковий вісник Ужгородського Національного Університету. Серія: «Право». Вип. 67. 2021. С. 345-349.

7. Богуш В. М. Інформаційна безпека держави. Київ: МК-Прес, 2005. 431 с.

8. Брижко В. М. Особливості ознак та матеріальна специфічність у сфері інформаційного права // Інформація і право. 2015. № 1. С. 15–26.

9. Довгань О. Д. Сучасні інформаційні структури як компоненти інформаційної безпеки // Інформація і право. 2015. № 2(14). С. 111-120.

10. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс // Інформація і право. 2018. № 2 (25). С. 73-85.

11. Ільницький М. П. Правове забезпечення інформаційної безпеки у сфері державного управління // Науковий вісник Ужгородського національного університету. Серія: «Право». 2015. Вип. 34. Т. 2 . С. 84-86.

12. Кайку М. Фізика майбутнього / пер. з англ. А. Кам'янець. Львів: Літопис, 2013. 432 с.

13. Калюжний Р. Питання концепції реформування інформаційного законодавства України // Правове, нормативне та метрологічне забезпечення системи інформації в Україні: тематичний збірник праць учасників Другої науково-технічної конференції. Київ, 2000. С. 17-21.

14. Климчук О. О., Ткачук Н. А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки // Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С. 75–83.

15. Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США): автореф. дис ... канд. політ. наук: спец. 21.01.01 / Нац. ін-т стратег. дослідж. Київ, 2005. 20 с.

16. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2003. 472 с.

17. Кунєв Ю. Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження // Юридичний вісник. 2021. 1 (58). С. 95-102.

18. Ліпкан В. А. Національна безпека України: навч. посіб. 2-ге вид. Київ, 2009. 576 с.

19. Ліпкан В. А., Харченко Л. С., Логінов О. В. Інформаційна безпека України: глосарій. Київ: Текст, 2004. 136 с.

20. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. … канд. юрид. наук. Київ, 2007.

21. Наливайко Л. М. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект // Вісник Запорізького державного університету. Серія: «Юридичні науки». 2003. № 1. С. 60–65.

22. Новицька Н. Б. Правове забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави. 2009. № 1. С. 44-47.

23. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в України // Право і суспільство. 2012. № 3. С. 132-137.

24. Орлов П. І. Правове забезпечення інформаційної безпеки // Вісник Харківського національного університету внутрішніх справ. 2001. Вип. 15. С. 96-99.

25. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України // Політичний менеджмент. 2008. № 4. С. 135-141.

26. Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці в інформаційній сфері // Вісник Національної академії правових наук України. 2014. № 3 (78). С. 43-52.

27. Пилипчук В. Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми // Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти: матеріали наук-практ. конф. (6 жовтня 2016 р., м. Київ). Київ: НТУУ «КПІ ім. Ігоря Сікорського», Вид-во «Політехніка», 2016. С. 24-28.

28. Писаренко Т. В., Кваша Т. К. Стан інноваційної діяльності та діяльності у сфері трансферу технологій в Україні у 2018 році: аналітична довідка. Київ: УкрІНТЕІ, 2019. 80 с.

29. Політанський В. С. Світові моделі та фундаментальні принципи інформаційного суспільства // Науковий вісник Ужгородського національного університету. Серія «Право». 2017. Вип. 43. Т. 1. С. 34–39.

30. Почепцов Г. Г. Інформаційна політика: навч. посіб. Київ: Знання, 2006. 211 с.

31. Почепцов Г. Г. Інформаційна політика та інформаційні війни: навч.-метод. посіб. Київ: Вид-во НАДУ, 2012. 120 с.

32. Скалацький В. М. Інформаційне суспільство: сучасні теорії та моделі (соціальнофілософський аналіз): дис.: спец. 09.00.03. Київ: Київ. нац. ун-т ім. Тараса Шевченка, 2006. 181 с.

33. Сливка М. М., Лук'янова Г. Ю. Правове забезпечення інформаційної безпеки: досвід країн Європейського Союзу // Юридичний науковий електронний журнал. № 11. 2021. С. 514-516.

34. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України: дис. ... д-ра політ. наук: спец. 23.00.02. / Одес. нац. юрид. акад. Одеса, 2005. 264 с.

35. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія. Київ: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

36. Тихомирова Є. Б., Смик Р. П. Інформаційна політика Польщі // Сучасні проблеми гуманітаристики: світоглядні пошуки, комунікативні та педагогічні стратегії: матеріали V Всеукраїнської науково-практичної конференції. Рівне, 2015. С. 113–115.

37. Чорнолуцький Р. Органи виконавчої влади України як суб'єкти нормопроєктної діяльності: концептуальні підходи до визначення // Наукові записки Інституту законодавства Верховної Ради України. 2016. № 1. С. 61–72.

38. Шмідт Е., Коен Д. Новий цифровий світ / пер. з англ. Г. Лелів. Львів: Дітопис, 2015. 304 с.