Принципи та методи удосконалення правового забезпечення інформаційної безпеки в сучасному вимірі

Леонтій Чистоклетов[1], Ростислав Буняк[2]

Опубліковано	Секція	УДК
30.07.2025	Право	342.9

DOI: https://doi.org/10.5281/zenodo.16897224

Анотація. У статті досліджено актуальні принципи та методи удосконалення правового забезпечення інформаційної безпеки в умовах цифрової трансформації. Акцентовано увагу на необхідності переосмислення традиційних підходів до формування правових норм у сфері інформаційних технологій з огляду на стрімкий розвиток штучного інтелекту, інтернету речей, хмарних обчислень і кіберзагроз.

Автором, на підставі теоретико-правового аналізу, запропоновано класифікацію принципів правового забезпечення інформаційної безпеки, зокрема принципи правомірності, технологічної нейтральності, превентивності, пропорційності та адаптивності. Крім того, розглянута у правовому регулюванні інформаційної безпеки специфіка використання принципів обґрунтованості та своєчасності захисту інформації, а також принципу прогнозу.

Із точки зору інформаційної політики в умовах російсько-української війни, спираючись на наукові погляди вітчизняних вчених, визначено принципи: системності та об'єктивності подання інформації; отримання балансу інтересів забезпечення свободи слова та прав і законних інтересів особи, суспільства і держави, їх взаємної відповідальності; гарантування забезпечення персональних даних та прав, пов'язаних з їх обігом; контрольованості та вибірковості розповсюдження «чуттєвої» інформації; захисту національних інтересів, зокрема у сфері інформаційної безпеки; забезпечення системності та координації дій органів державного управління і регулювання в інформаційній сфері; забезпечення охорони і захисту інформації, зокрема запобігання відповідно до закону розголошенню інформації з обмеженим доступом (принцип дотримання вимог державної та військової таємниці); недопущення зловживання свободою діяльності засобів масової інформації на шкоду правам і свободам людини.

З метою удосконалення правового забезпечення інформаційної безпеки, визначено методи нормативно-правової модернізації, серед яких - гармонізація національного законодавства з міжнародними стандартами, впровадження risk-based regulation, посилення відповідальності за порушення інформаційної безпеки, а також розвиток soft law інструментів. Окрему увагу приділено проблемам правової визначеності у сфері обігу інформації, персональних даних і кібербезпеки.

[1] професор кафедри адміністративного та інформаційного права, Навчально-наукового інституту права, психології та інноваційної освіти Національного університету "Львівська політехніка", доктор юридичних наук, професор ORCID iD: 0000-0002-3306-1593

[2] здобувач другого (магістерського) рівня вищої освіти Навчально-наукового інститут права, психології та інноваційної освіт Національного університету "Львівська політехніка" ORCID iD: 0009-0002-7685-3539

Обґрунтовано доцільність міждисциплінарного підходу до формування інформаційної політики держави з урахуванням прав людини, інтересів бізнесу та вимог національної безпеки.

Зроблено висновок про необхідність розробки гнучкої та динамічної нормативної бази, здатної оперативно реагувати на виклики інформаційного суспільства та забезпечувати ефективну правову охорону інформаційного простору.

Ключові слова: інформаційна безпека, правове забезпечення, принципи права, методи регулювання, цифрова трансформація, кібербезпека, нормативно-правова модернізація, міжнародні стандарти, персональні дані, інформаційна політика.

Principles and methods of improving legal 5 ensurance of information security in the modern dimension

Abstract. The article examines current principles and methods for improving the legal support of information security in the context of digital transformation. The emphasis is on the need to rethink traditional approaches to the formation of legal norms in the field of information technologies given the rapid 33 development of artificial intelligence, the Internet of Things, cloud computing, and cyber threats.

The author, based on theoretical and legal analysis, proposed a classification of 5 principles of legal support for information security, in particular the principles of legality, technological neutrality, prevention, proportionality, and adaptability. In addition, the specifics of using the principles of reasonableness and timeliness of information protection, as well as the principle of forecasting, in the legal regulation of information security are considered.

From the point of view of information policy, the implementation of which is carried out in the conditions of the Russian-Ukrainian war, based on the scientific views of domestic scientists, the principles of: systematic and objective presentation of information; achieving a balance of interests in ensuring freedom of speech and rights and legitimate interests of the individual, society and the state, their mutual responsibility; guaranteeing the provision of personal data and rights related to their circulation; controllability and selectivity of the distribution of "sensitive" information; protection of national interests, in particular in the field of information security; ensuring the consistency and coordination of actions of state administration and regulatory bodies in the information sphere; ensuring the protection and security of information, in particular preventing the disclosure of information with restricted access in accordance with the law (the principle of compliance with the requirements of state and military secrets); preventing abuse of freedom of the media to the detriment of human rights and freedoms.

In order to improve the legal support of information security, methods of regulatory modernization were considered, including the harmonization of national legislation with international standards, the introduction of risk-based regulation, increased liability for information security violations, and the development of soft law instruments. Special attention is paid to the problems of legal certainty in the field of information circulation, personal data and cybersecurity.

The feasibility of an interdisciplinary approach to the formation of the state's information policy, taking into account human rights, business interests, and national security requirements, is substantiated.

The conclusion is made about the need to develop a flexible and dynamic regulatory framework capable of promptly responding to the challenges of the information society and ensuring effective legal protection of the information space.

Keywords: information security, legal support, principles of law, methods of regulation, digital transformation, cybersecurity, regulatory modernization, international standards, personal data, information policy.

Вступ

Постановка проблеми. У сучасному глобалізованому світі інформаційна безпека набуває статусу одного з ключових елементів національної, публічної та приватної безпеки. Стрімкий розвиток інформаційно-комунікаційних технологій, поширення цифрових сервісів, зростання обсягу оброблюваних персональних та конфіденційних даних, а також зростаюча кількість кіберзагроз і атак на критичну інфраструктуру обумовлюють необхідність постійного вдосконалення правового механізму захисту інформаційного простору. Однак чинна система правового забезпечення інформаційної безпеки не встигає за темпами технологічного розвитку, що створює численні прогалини у правовому полі, знижує ефективність протидії кіберзагрозам і ускладнює забезпечення балансу між правами людини, інтересами держави та вимогами бізнесу.

Складність проблеми також полягає в багатовимірності інформаційної безпеки як об'єкта правового регулювання, яка охоплює такі сфери, як захист персональних даних, таємниці комунікацій, інтелектуальної власності, інформаційного суверенітету, а також безпеку критичних інформаційних інфраструктур. Відсутність системного, узгодженого і гнучкого підходу до регулювання цих питань ускладнює правозастосування та створює ризики як для громадян, так і для органів влади. Застарілість окремих нормативноправових актів, їхня фрагментарність і нечіткість формулювань призводять до правової невизначеності, що у свою чергу є фактором зниження довіри до держави та її інституцій у сфері кіберрегулювання.

У цьому контексті актуалізується потреба у переосмисленні засадничих принципів правового регулювання інформаційної безпеки, що має включати технологічну нейтральність, правомірність, пропорційність та адаптивність. Одночасно постає питання ефективного добору методів удосконалення правового забезпечення, зокрема - шляхом імплементації міжнародних стандартів, розвитку гнучких регуляторних моделей (зокрема soft law), застосування risk-based підходів до оцінки загроз, а також посилення правової відповідальності за порушення норм інформаційної безпеки.

Метою статті є комплексне дослідження принципів та методів удосконалення правового забезпечення інформаційної безпеки в умовах трансформації інформаційного суспільства та загострення кіберзагроз.

Аналіз дослідження проблеми. Проблема правового забезпечення інформаційної безпеки не є новою для вітчизняного та зарубіжного правознавства, однак у сучасних умовах вона набула якісно нового змісту. Аналіз наукових джерел, зокрема А.Г. Арсеєнко, М.В. Банчук, М. Т. Гаврильців, О.І. Доронін, Ю.І. Когут, Б.А. Кормич, І.Б. Лук'янець та багатьох інших науковців , свідчить, що впродовж останнього десятиліття спостерігається посилення інтересу до цієї тематики в контексті цифрової трансформації, глобалізації кіберпростору, гібридних загроз і збільшення випадків порушення інформаційної недоторканності. Разом із тим, більшість досліджень залишаються недостатньо визначеними, орієнтованими на окремі аспекти, зокрема захист персональних даних, кіберзлочинність чи інформаційний суверенітет, при цьому комплексне бачення дієвих принципів і методів в удосконаленні правового забезпечення інформаційної безпеки зустрічається рідко.

Результати

Правове забезпечення інформаційної безпеки охоплює систему норм, принципів, інститутів та механізмів, спрямованих на врегулювання суспільних відносин у сфері захисту інформації, інформаційних ресурсів, систем та комунікаційних мереж. У сучасних умовах це регулювання має враховувати як швидкі темпи цифровізації, так і динаміку кіберзагроз, що вимагає нової якості правового реагування.

У правовій доктрині інформаційна безпека трактується як комплексна правова категорія, що охоплює елементи публічного і приватного права, зокрема адміністративного, інформаційного, конституційного, кримінального та міжнародного. Її основою є сукупність норм, які регулюють діяльність державних органів, суб'єктів господарювання та громадян у сфері створення, обробки, зберігання, передачі та захисту інформації [1, с. 256].

Сутність інформаційної безпеки полягає не лише у протидії інформаційним загрозам, але й у створенні умов для реалізації інформаційних прав і свобод, дотримання правових гарантій доступу до публічної інформації, а також захисту персональних даних. З огляду на це, забезпечення інформаційної безпеки потребує балансування між інтересами безпеки та правами людини, що зумовлює необхідність чіткого правового регулювання цієї сфери.

У нормативно-правовому полі України визначення поняття «інформаційна безпека» закріплено, зокрема, у 13 Законі України «Про національну безпеку України», де вона розглядається як захищеність життєво важливих інтересів людини, суспільства і держави, що унеможливлює заподіяння шкоди в інформаційній сфері. У контексті цього визначення інформаційна безпека охоплює такі аспекти, як безпека інформаційної інфраструктури, протидія кібератакам, захист від дезінформації, забезпечення інформаційного суверенітету, а також формування стійкого до маніпуляцій громадського простору [2].

Інформаційна безпека не обмежується виключно технічними аспектами кіберзахисту або контролем за комунікаційними каналами - вона охоплює широкий спектр політичних, правових, соціальних, культурних, морально-етичних та технологічних елементів, які впливають на функціонування держави та життєдіяльністьгромадян.

Саме тому сучасні наукові підходи трактують інформаційну безпеку як системну категорію, що забезпечує стабільний розвиток держави, збереження її суверенітету, територіальної цілісності, захист прав та свобод громадян в умовах інформаційного суспільства [3, с. 59].

У структурі національної безпеки інформаційна безпека виконує роль базового гаранта стійкості демократичної системи до зовнішніх та внутрішніх дестабілізуючих впливів. Вона є критично важливою в контексті ведення гібридних воєн, коли традиційні форми військових дій доповнюються масштабними інформаційно-психологічними операціями, спрямованими на деморалізацію населення, дезорієнтацію політичного керівництва, руйнування довіри до державних інституцій і посилення соціальної напруги. Так, у зв'язку прийняття скандального Закону №12414 про діяльність НАБУ і САП, "що нівелює незалежність цих органів" [4] та "втратою інституціональної незалежності через контроль Генпрокурором підслідності та можливості передоручення повноважень прокурорів САП іншим прокурорам" [5], за прогнозом Центру протидії дезінформації РНБО в найближчі два тижні російська пропаганда посилить використання теми мітингів в Україні у своїх інформаційних кампаніях. Очікується, що ворожі ресурси поширюватимуть неправдиві твердження, що український народ нібито вимагає "капітуляції", "повалення влади" та "припинення війни будь-якою ціною" [6].

Отже, в наслідок інформаційного тиску, маніпуляцій, кібератак та дезінформаційних кампаній, які ведуться системно, із залученням значних технологічних та людських ресурсів, сьогодні Україна, як держава, що перебуваючи у стані збройного конфлікту з російською федерацією, особливо гостро потребує комплексного забезпечення реалізації дієвих принципів і методів в удосконаленні правового регулюванні вітчизняного інформаційного простору. У цьому контексті інформаційна безпека виступає не лише як елемент оборонної доктрини, але і як

інструмент формування свідомості, національної ідентичності, громадянської стійкості до зовнішніх впливів.

В. Ліпкан зазначає, що інформаційна безпека України є органічною складовою національної, відтак її розгляд є необхідним для формування базових знань та уявлень про національну безпеку. Нормальна життєдіяльність суспільства визначається рівнем розвитку, якістю функціонування і безпекою інформаційного середовища, а також рівнем і станом нормативно-правового забезпечення даних процесів. Інформаційне законодавство спрямоване на закріплення державної інформаційної політики, яка передбачає забезпечення гарантованого рівня національної безпеки в інформаційній сфері, нормального розвитку інформаційних технологій і засобів захисту інформації, виключення монополізму в даній області, запобігання розроблення інформаційно деструктивних технологій впливу на антропогенну популяцію, захист авторських і суміжних прав тощо [7, 1 с. 194].

З точки зору адміністративного та інформаційного права, інформаційна безпека визначає правову природу багатьох процесів, пов'язаних із забезпеченням законного обігу інформації, захистом персональних даних, недопущенням поширення інформації, що становить загрозу національним інтересам, та регулюванням діяльності суб'єктів інформаційного простору - медіа, провайдерів, державних органів. Закони та підзаконні акти, що регулюють цю сферу, визначають не лише права і обов'язки учасників інформаційних правовідносин, але і встановлюють правові механізми виявлення, реагування та нейтралізації загроз, що мають інформаційне походження [8, с. 91].

Інформаційна безпека вимагає постійного нормативного оновлення - у відповідь на технологічний розвиток (зокрема, у сфері штучного інтелекту, big data, deep fake, блокчейну) та нові форми загроз, які виявляються на стику інформаційних, соціальних та політичних процесів. Водночас адміністративно-правові механізми управління інформаційною безпекою повинні передбачати баланс між національними інтересами та фундаментальними правами людини, зокрема правом на свободу вираження поглядів, доступ до інформації 3та захист персональних даних.

Окрему увагу слід приділити ролі інформаційної безпеки у процесі стратегічного планування національної безпеки. У ключових державних документах, таких як Стратегія національної безпеки України, Стратегія кібербезпеки, Концепція розвитку сектора безпеки і оборони, інформаційна безпека визнається пріоритетним напрямом державної політики.

Це свідчить про усвідомлення владою природи новітніх загроз та необхідності вибудови інституційної вертикалі, спроможної протистояти гібридному тиску. Проте, реальна ефективність інформаційної безпеки залежить не лише від юридичних декларацій чи технічного оснащення, а й від рівня медіаграмотності населення, довіри до інформаційних джерел, наявності етичних стандартів у журналістиці, а також готовності суспільства до консолідації навколо національних інтересів.

Важливими є також міжнародні аспекти, оскільки Україна активно взаємодіє з НАТО, ЄС та іншими міжнародними організаціями у сфері кіберзахисту, обміну інформацією, спільного реагування на дезінформацію та захисту інформаційного суверенітету. Це дозволяє не лише підвищити національну спроможність у сфері інформаційної безпеки, а й інтегруватися у систему колективної безпеки демократичного світу [8, с. 94].

Одним з ключових напрямів удосконалення правового забезпечення інформаційної безпеки є формулювання та впровадження оновлених принципів правового регулювання. Для забезпечення рівноправного та скоординованого включення України до світового інформаційного простору необхідно визначити головні принципи міжнародної взаємодії в цій сфері, до яких можна віднести: використання

світового досвіду з інтеграції правового, організаційного і технічно-технологічного змісту; створення нормативно-правової бази інформатизації різних суб'єктів на основі системи двох- і багатосторонніх міжнародних договорів й угод; правове і технологічне забезпечення доступу різних суб'єктів до закордонних інформаційних ресурсів; упровадження міжнародних стандартів для забезпечення пошуку, збирання, збереження і використання інформації; активне використання закордонних інформаційних продуктів для формування власних інформаційних ресурсів України; придбання ліцензій; забезпечення актуальності інформаційних ресурсів України і збільшення національної присутності у світовому інформаційному просторі; забезпечення участі України як повноправного члена міжнародних програм і проєктів у зв'язку з формуванням світового інформаційного простору, створенням нових інформаційних технологій; моніторинг форм і методів впливу міжнародних засобів комунікацій на процеси формування суспільної свідомості в Україні [9, с. 136].

Існують інші моделі класифікації принципів правового регулювання інформаційної безпеки. Так, М.В. Баран до зазначеної системи принципів виділяє принцип обґрунтованості та своєчасності захисту інформації, а також принцип прогнозу. Принцип обґрунтованості, на думку автора, виходячи з балансу життєво важливих інтересів особи, суспільства, держави, полягає у встановленні шляхом експертної оцінки доцільності обмеження доступу до конкретної інформації, виділення ймовірних економічних і інших наслідків цього акту. Принцип своєчасності захисту інформаційної сфери дозволяє реалізувати процедуру попереднього обмеження доступу до інформації, що захищається, і полягає у встановленні обмежень на поширення інформації з моменту отримання, розробки або завчасно. Принцип прогнозу інформаційної безпеки спрямований на захист безпеки від зовнішніх і внутрішніх загроз у інформаційній сфері. Базується на об'єктивній, реальній оцінці об'єктів, що охороняються – інформації, інфраструктури, суб'єктів, пов'язаних зі створенням, перетворенням, споживання інформації; моделюванні можливої протиправної діяльності, що зазіхає на інформаційну безпеку [10, с.132].

Із точки зору інформаційної політики в умовах російсько-української війни, Н. Б. Новицька, О.О. Пунда та О.Д. Добрянська, до принципів правового регулювання відносять:

- системность та об'єктивность подання інформації;
- отримання балансу інтересів забезпечення свободи слова та прав і законних інтересів особи, суспільства і держави, їх взаємної відповідальності;
- гарантування забезпечення персональних даних та прав, пов'язаних з їх обігом;
- контрольованості та вибірковості розповсюдження «чуттєвої» інформації;
- захисту національних інтересів, зокрема у сфері інформаційної безпеки;
- забезпечення системності та координації дій органів державного управління і регулювання в інформаційній сфері;
- забезпечення охорони і захисту інформації, зокрема запобігання відповідно до закону розголошенню інформації з обмеженим доступом (принцип дотримання вимог державної та військової таємниці);
- недопущення зловживання свободою діяльності засобів масової інформації на шкоду правам і свободам людини [11, с. 75].

На підставі вище вказаного, на нашу думку, класифікація принципів правового забезпечення інформаційної безпеки повинна включати:

- принцип правомірності - забезпечення відповідності всіх дій у сфері інформаційної безпеки нормам права, із дотриманням фундаментальних прав і свобод людини;
- принцип технологічної нейтральності - розробка норм, що не прив'язані до конкретних технологій, з метою забезпечення їхньої універсальності та стійкості

до
змін;

- принцип превентивності - орієнтація не лише на реагування, а й на запобігання інформаційним загрозам через прогностичне законодавство і системи раннього виявлення;
- принцип пропорційності - дотримання балансу між заходами державного втручання та рівнем загроз, недопущення надмірного обмеження прав громадян;
- принцип адаптивності - здатність нормативно-правової системи оперативно змінюватися відповідно до нових викликів, включно з механізмами перітичного перегляду законодавства.

Методи вдосконалення правового забезпечення, у свою чергу, можуть бути поділені на кілька рівнів. На нормативному рівні актуальним є ухвалення базового законодавчого акта, який би комплексно врегулював питання інформаційної безпеки з урахуванням усіх категорій суб'єктів - держави, бізнесу та громадян. Необхідним є також гармонізація національного законодавства з міжнародними стандартами, що передбачає адаптацію до положень таких документів, як GDPR, Директива NIS2, Будапештська конвенція про кіберзлочинність тощо [12, с. 28].

На інституційному рівні варто посилити координацію між органами державної влади, зокрема шляхом створення єдиного координаційного центру з кібербезпеки, який би забезпечував моніторинг загроз, обмін інформацією між суб'єктами та формування рекомендацій щодо правового реагування.

Окремої уваги заслуговує впровадження soft law інструментів: кодексів поведінки, рекомендацій, стандартів діяльності для приватних гравців ринку IT, які можуть діяти як додаткові регулятивні важелі без потреби у жорсткому законодавчому втручанні. Такий підхід дозволяє оперативно реагувати на зміни технологій та швидко поширювати найкращі практики.

Ще одним методологічним напрямом захисту інформаційного простору є розвиток системи правової відповідальності за порушення у сфері інформаційної безпеки. Це стосується не лише кримінальної, а й адміністративної та цивільно-правової відповідальності, які мають бути чітко розмежовані та ефективно реалізовані. Важливо при цьому враховувати особливості об'єктів правової охорони (персональні дані, комерційна таємниця, об'єкти критичної інфраструктури тощо) та потенційні наслідки їх порушення.

Як зазначає В.В. Шемчук, особливе значення у процесі вдосконалення правового забезпечення інформаційної безпеки відіграє метод міждисциплінарного підходу. При цьому, інформаційна безпека не є суто юридичною категорією - вона лежить на перетині права, інформаційних технологій, соціології, психології, управління ризиками та національної безпеки. Це зумовлює необхідність формування політики у цій сфері з урахуванням аналітичних даних, технічних параметрів інформаційних систем, а також соціокультурного контексту. Такий підхід дозволяє розробляти не лише нормативно-правові акти, але й програми освіти, протоколи реагування на інциденти, стандарти для корпоративного сектору та міждержавні угоди, які у своїй сукупності створюють цілісну систему правової підтримки інформаційної безпеки [13, с. 287].

Важливо також наголосити на потребі в інституційній модернізації, яка включає реформування вже існуючих органів кібербезпеки, удосконалення їхньої взаємодії, а також підвищення спроможності судових та правоохоронних інституцій у сфері розгляду кіберінцидентів. На практиці часто виникає проблема відсутності належної кваліфікації або інструментів для правової оцінки таких інцидентів, що спричиняє затримки у розслідуваннях, складнощі у доказуванні та ухилення від відповідальності. У цьому контексті варто розглядати запровадження спеціалізованих судів або судових палат з питань цифрових прав та інформаційної безпеки. Не менш важливою складовою

є правова просвіта та цифрова грамотність як населення, так і представників державного сектору. Недостатній рівень обізнаності про базові принципи інформаційної безпеки з боку користувачів та посадових осіб призводить до нехтування заходами захисту, що, в свою чергу, ускладнює забезпечення правового порядку. У зв'язку з цим доцільним є включення елементів правової культури у сфері інформації до освітніх програм на різних рівнях, а також активізація публічно-правових Зкампаній з метою підвищення рівня обізнаності щодо відповідальності за кіберзлочини та інші правопорушенняу цифровому середовищі [1, с. 304].

Також слід приділити увагу інноваційним підходам до правового моніторингу, зокрема - використанню алгоритмічного аналізу нормативно-правових актів, прогнозуванню юридичних наслідків нових технологій, а також цифровізації самої регуляторної діяльності (RegTech). Такі інструменти здатні підвищити ефективність оцінки
нормативного впливу, виявляти правові колізії ще на етапі проєктування актів та сприяти створенню адаптивного цифрового правового середовища.

Таким чином, основним завданням на сучасному етапі є формування гнучкої, інтегрованої та багаторівневої системи правового забезпечення інформаційної безпеки, здатної забезпечити стабільність правового порядку у сфері цифрових технологій, не обмежуючи при цьому інноваційного розвитку та прав громадян на інформаційну свободу.

У світлі геополітичної нестабільності та воєнної агресії російської федерації проти України питання інформаційного суверенітету набуває особливої актуальності. Йдеться не лише про технічну здатність захищати національний інформаційний простір, але й про правову автономність у сфері регулювання цифрової діяльності. Власна нормативна база, незалежна інфраструктура (включно з центрами обробки даних, захищеними каналами зв'язку), а також законодавчо підтримувана політика щодо пріоритету національних інформаційних інтересів мають стати стратегічним пріоритетом. Відповідно, необхідно формулювати нормативне визначення поняття «інформаційний суверенітет», передбачити спеціальні юридичні режими для захисту критичних даних та забезпечити прозору модель контролю іноземних суб'єктів у сфері ІКТ [14, с. 156].

У правовому регулюванні інформаційної безпеки здатність інформаційного суверенітету спрямоване на державне формування та регулювання національного інформаційного простору від зовнішнього та внутрішнього впливу на національну безпеку.

Поняття «інформаційного суверенітету» дедалі частіше використовується в сучасній юридичній науці та політичному дискурсі, особливо в умовах зростання гібридних загроз, кібершпигунства, зовнішнього втручання в інформаційний простір та підриву інформаційної стабільності держави [9, с. 136].

З правової точки зору інформаційний суверенітет можна розглядати як розширення класичного поняття державного суверенітету на сферу інформаційних відносин. Він включає як негативний компонент - право держави на обмеження втручання зовнішніх сил в її інформаційний простір, так і позитивний аспект - зобов'язання формувати правові та інституційні засади для розвитку внутрішніх інформаційних систем, цифрового контенту, телекомунікаційної інфраструктури та безпеки даних. Зокрема, йдеться про наявність власного нормативного регулювання щодо хмарних обчислень, баз даних, інтернет-сервісів, засобів масової інформації, а також платформ, що поширюють інформацію серед масової аудиторії.

У межах інформаційного суверенітету особливу роль відіграє національний контроль над критичною інформаційною інфраструктурою (далі - КІІ), до якої належать енергетичні, фінансові, транспортні та урядові цифрові системи. Їхнє захоплення або

паралізація потенційно може спричинити катастрофічні наслідки для державної безпеки, тому законодавство має передбачати спеціальні режими доступу до КІІ, обмеження для іноземних постачальників ПЗ та хмарних сервісів, а також обов'язковість локалізації стратегічних даних на території України.

Таким чином, концепція інформаційного суверенітету потребує чіткого нормативного закріплення у національному законодавстві як самостійної правової категорії. Це дозволить не лише структуризувати державну політику у сфері інформаційної безпеки, але й ефективно взаємодіяти з міжнародними партнерами на умовах рівноправності, взаємної відповідальності у цифровому просторі, із запровадженням сучасних принципів та методів правового регулювання інформаційного простору.

Висновки

Узагальнюючи результати дослідження, можна констатувати, що правове забезпечення інформаційної безпеки в сучасних умовах є багатовимірною, динамічною та складною сферою, яка потребує системного, міждисциплінарного й адаптивного підходу. З огляду на стрімкий розвиток інформаційних технологій, зростання кількості та складності кіберзагроз, а також посилення ролі цифрового середовища в усіх сферах суспільного життя, традиційні моделі правового регулювання виявляються недостатніми. Саме тому першочерговим завданням є переосмислення базових принципів інформаційної безпеки, їх актуалізації, відповідно до вимог цифрової доби, а також інституційного, нормативного та технологічного оновлення регуляторної політики в цій сфері. Значущу роль у цьому контексті відіграють принципи превентивності, технологічної нейтральності, пропорційності, правомірності та адаптивності, які мають стати методологічною основою сучасного інформаційного права.

Аналіз чинного законодавства та міжнародного досвіду свідчить про необхідність комплексного перегляду методів правового впливу на інформаційні процеси. Це включає розробку нових законодавчих актів із чітко визначеним предметом регулювання, запровадження гнучких механізмів правового моніторингу, удосконалення режимів відповідальності за правопорушення у сфері інформації, а також зміцнення інституційної спроможності суб'єктів, відповідальних за безпеку цифрового простору. Особливої актуальності набуває питання формування концепції інформаційного суверенітету як стратегічної 8 основи державної політики у сфері інформаційної безпеки. Забезпечення контролю над критичною інформаційною інфраструктурою, запобігання зовнішньому втручанню в національний інформаційний простір, нормативне закріплення пріоритетності національних інтересів у цифровій сфері - усе це вимагає чітко сформульованих правових норм, узгоджених із міжнародними стандартами, орієнтованих на реальні безпекові виклики, з якими стикається Україна.

Таким чином, удосконалення правового 8 забезпечення інформаційної безпеки має здійснюватися на основі цілісного принципового та методологічного підходу, який передбачає не лише оптимізації формальних норм, а й розвиток інституційної культури, підвищення правової грамотності, зміцнення міжнародного співробітництва та впровадження інноваційних правових технологій.

Список використаних джерел

1. Бєлай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою
держави. Київ : Національна академія Служби безпеки України, 2018. 408 с.

2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 11.07.2025).
3. Панченко О. З Інформаційна безпека держави як елемент соціокультури. Аспекти публічного управління. 2020. No1. С. 9 58-67.
4. Зеленський підписав скандальний закон №12414.URL: https://www.bbc.com/ukrainian/articles/cgeqllep70no (дата звернення: 26.07.2025).
5. Кінець епохи незалежних антикорупціонерів: прихована правда за новим законом. URL: https://jurliga.ligazakon.net/analitycs/237879_knets-epokhi-nezalezhnikh-antikoruptsonerv-prikhovana-pravda-za-novim-zakonom (дата звернення: 29.07.2025).
6. Російська пропаганда готує нові інформаційні атаки на Україну - ЦПД РНБО. URL: https://unn.ua/news/rosiiska-propahanda-hotuie-novi-informatsiini-ataky-na-ukrainu-tspd-rnbo (дата звернення: 29.07.2025).
7. Ліпкан В.А. Національна безпека України: Навч. посіб. 2-ге вид. К., 2009. с. 576.
8. Ткачук Т.Ю., Довгань О.Д. Система 3 інформаційної безпеки України: онтологічні14 виміри. Інформація і право. 2018. No 1 9 (24). 14 С. 14 89–104.
9. Солодка О. Пріоритетні напрями забезпечення інформаційного суверенітету України. Науковий вісник Ужгородського Національного Університету. 2024. Т. 85. С. 134–138.
10. Баран М.В. Принципи правового регулювання інституту інформаційної безпеки. Науковий вісник Ужгородського Національного Університету, 2021. Серія ПРАВО. Випуск 66.
11. Новицька Н. Б., Пунда О.О., Добрянська О.Д. Принципи інформаційної політики в умовах війни та їх нормативно-правове закріплення. Соціологія права. Випуск 1–2 (40–41), 2022. С. 75. https://elar.khmnu.edu.ua/server/api/core/bitstreams/8f9ec4e4-f843-4b9e-b37a-e93d379d7898/content. (дата звернення: 20.07.2025).
12. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26–37.
13. Шемчук В.В. Загрози інформаційній безпеці: проблеми визначення та подолання. Експерт: парадигми юридичних наук і державного управління. 2020. No 1(7). С. 285–296.
14. Рак А., Прончук Д. Комплексна модель управління інформаційною безпекою та розрахунок її ефективності. Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2024). Тернопіль, 2024. С.156-157.