УДК 004.056.53
DOI https://doi.org/10.32782/2524-0374/2024-10/76

МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

MECHANISM FOR ENSURING INFORMATION SECURITY OF THE STATE

Шевчук М.О., к.ю.н.,
докторант кафедри конституційного, адміністративного та фінансового права
Хмельницький університет управління та права імені Леоніда Юзькова

Інформаційна безпека держави в сучасному світі відіграє ключову роль в забезпеченні її національної безпеки. Ця стаття присвячена дослідженню механізмів забезпечення інформаційної безпеки держави. У статті розглядаються теоретичні підходи до захисту інформаційних ресурсів, основні загрози інформаційній безпеці, а також технологічні, правові та організаційні аспекти забезпечення інформаційної безпеки. Дослідження розглядає інформаційну безпеку як багатогранне явище, що охоплює не лише технологічний захист, але й правові, організаційні та соціальні аспекти. Зі стрімким розвитком цифрових технологій та активним використанням інформаційних систем у всіх сферах життєдіяльності суспільства, виникають нові виклики, що вимагають негайних та швидких дій з боку державних інституцій. Інформаційна безпека охоплює захист інформаційних ресурсів держави від несанкціонованого доступу, викрадення, спотворення або знищення. Втрата інформації або компрометація даних може призвести до серйозних наслідків для національної безпеки, економіки та стабільності суспільства. Тому питання забезпечення інформаційної безпеки має бути одним із пріоритетів державної політики. Створення розвиненого та захищеного середовища є головною умовою розвитку суспільства та конкурентоспроможності держави. Ефективна система заходів щодо забезпечення інформаційної безпеки громадян, суспільства та держави дає можливість вчасно попереджати та виявляти потенційні й реальні загрози національним інтересам і запобігати збиткам у соціально економічній сфері. Також у статті подано всебічний аналіз проблем забезпечення інформаційної безпеки держави. Дослідження є актуальним у контексті зростання кіберзагроз та необхідності забезпечення стійкості критичної інфраструктури. На основі дослідження запропоновано рекомендації щодо покращення державної політики у сфері інформаційної безпеки. Окрім того, особлива увага приділяється необхідності міжнародного співробітництва та розробки ефективних стратегій для підвищення кіберстійкості державних інституцій. Новизна дослідження полягає у комплексному аналізі взаємозв'язку між різними аспектами інформаційної безпеки та розробці практичних рекомендацій, які можуть бути використані для розробки ефективних стратегій захисту інформаційних ресурсів на різних рівнях.

Ключові слова: інформація, державна безпека, інформаційні ресурси, кібербезпека, кіберстійкість, кібертероризм, механізми захисту, міжнародне співробітництво, інформаційна стратегія.

Information security of the state in the modern world plays a key role in ensuring its national security. This article is devoted to the study of mechanisms for ensuring information security of the state. The article discusses theoretical approaches to the protection of information resources, the main threats to information security, as well as technological, legal and organizational aspects of information security. The study considers information security as a multifaceted phenomenon, covering not only technological protection, but also legal, organizational and social aspects. With the rapid development of digital technologies and the active use of information systems in all spheres of society, new challenges arise that require immediate and rapid action by state institutions. Information security covers the protection of information resources of the state from unauthorized access, theft, distortion or destruction. Loss of information or compromise of data can lead to serious consequences for national security, economy and stability of society. Therefore, the issue of ensuring information security should be one of the priorities of state policy. The creation of a developed and protected environment is the main condition for the development of society and the competitiveness of the state. An effective system of measures to ensure the information security of citizens, society and the state makes it possible to timely prevent and identify potential and real threats to national interests and prevent losses in the socio-economic sphere. The article also presents a comprehensive analysis of the problems of ensuring the information security of the state. The study is relevant in the context of the growth of cyber threats and the need to ensure the stability of critical infrastructure. Based on the study, recommendations for improving public policy in the field of information security have been proposed. In addition, special attention is paid to the need for international cooperation and the development of effective strategies to increase the cyber resilience of state institutions. The novelty of the study is a comprehensive analysis of the relationship between different aspects of information security and the development of practical recommendations that can be used to develop effective strategies for protecting information resources at different levels.

Key words: information, state security, information resources, cyber security, cyber resilience, cyberterrorism, protection mechanisms, international cooperation, information strategy.

Постановка проблеми. Основи правового механізму забезпечення інформаційної безпеки розкриваються неоднозначно. У великій чисельності джерел зазначено, що поняття «інформаційна безпека» виникає з появою засобів інформаційних комунікацій між людьми. Забезпечення інформаційної безпеки є найважливішою функцією держави, з огляду на те, що теоретичні основи правового забезпечення інформаційної безпеки підлягають більш точному визначенню та тлумаченню як у науковій літературі, так і на законодавчому рівні. Тенденція до збільшення відкритості суспільства, широке використання інформаційно-комунікаційних технологій створюють передумови для можливих протиправних дій відносно інформації, її користувачів, а також інформаційних систем зв'язку, що призводить до зниження рівня забезпечення інформаційної безпеки держави. На стан інформаційної безпеки впливають як внутрішні, так і зовнішні фактори: політична ситуація в державі й загалом у світі, загальний рівень економічного, соціального та інформаційного розвитку країни. Отже, потреба забезпечення національної безпеки належить до концептуальних основ діяльності суспільства. Усе це й зумовлює необхідність ґрунтовного дослідження категорії «механізм забезпечення інформаційної безпеки держави».

Аналіз останніх досліджень і публікацій. Проблематика забезпечення інформаційної безпеки складна і багатоаспектна, що зумовлює необхідність вивчення й узагальнення наукових праць представників різних галузей юридичної науки. Окремі аспекти правового регулювання інформаційної сфери стали об'єктом наукового аналізу в працях багатьох дослідників, зокрема В. А. Ліпкана, Ю. Є. Максименка, В. М. Желіховського, О. О. Золотаря, В. І. Волошина, В. П. Абрамова, С. О. Кондратьєва, Л. П. Марченка та ін.

Мета статті – метою даної статті є аналіз теоретичних основ і методології вивчення механізму забезпечення інформаційної безпеки, а також розкриття сутнісних ознак та особливостей окресленої категорії. Дослідження спрямоване на виявлення основних загроз інформаційній безпеці, оцінку впливу технологічних, правових та організаційних факторів на рівень захисту інформаційних ресурсів, а також на формулювання стратегій щодо підвищення кіберстійкості державних інституцій.

На цій підставі сформовано наступні завдання:

Аналіз теоретичних підходів до забезпечення інформаційної безпеки держави, визначення їх переваг та обмежень, а також вивчення загроз інформаційній безпеці, включаючи кіберзлочинність, шпигунство, саботаж та інші форми атак.

Оцінка сучасних кібератак та методів їх виявлення і протидії, зокрема використання сучасних технологій штучного інтелекту та машинного навчання, а також дослідження правових аспектів захисту інформаційних ресурсів, аналіз існуючого законодавства та пропозиції щодо його вдосконалення.

Розгляд організаційних заходів з забезпечення інформаційної безпеки, включаючи роль державних органів та приватного сектору.

Вивчення міжнародного співробітництва у сфері інформаційної безпеки, аналіз кращих практик та можливостей інтеграції національних стратегій з глобальними ініціативами, а також формулювання рекомендацій щодо покращення державної політики у сфері інформаційної безпеки на основі проведеного аналізу.

Виклад основного матеріалу. У контексті дослідження, насамперед, необхідно з'ясувати зміст правової категорії «механізм забезпечення інформаційної безпеки» та визначити підхід українського законодавця до розуміння цієї категорії. Це дасть змогу комплексно та ґрунтовно розглянути структуру механізму забезпечення інформаційної безпеки держави, виявити причини недостатньої дієвості цього механізму загалом та окремих його елементів, зокрема. Науковці В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський використовують діяльнісний підхід до розуміння забезпечення інформаційної безпеки держави та зазначають, що забезпечення інформаційної безпеки досягають у процесі свідомої цілеспрямованої діяльності органів державного управління, із запобігання можливому порушенню їх нормального функціонування в результаті дії загроз і небезпек [1] .

Важливо зауважити, що законодавче визначення інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.»: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» (п. 13 Закону) [2].

Інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні та внутрішні чинники, найважливішими з яких є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична обстановка в державі. Водночас інформаційна безпека є складною, динамічною, цілісною соціальною системою, компонентами якої є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна інформаційна єдність останніх складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх конкурентоздатний, прогресивний розвиток [3, с. 154–155]. Забезпечення інформаційної безпеки завдяки послідовній реалізації грамотно сформульованої інформаційної стратегії значною мірою може сприяти забезпеченню досягнення успіху при вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Варто зазначити, що про необхідність захисту інформаційної безпеки наголошується в Конституції України: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» (ст. 17) [4].

Важливо зауважити, що існує кілька основних підходів до забезпечення інформаційної безпеки держави. Найбільш поширеними є технологічний, правовий та організаційний підходи. Кожен із них має свої специфічні особливості та застосовується залежно від характеру та джерела загроз.

Технологічний підхід ґрунтується на застосуванні сучасних інформаційних та комунікаційних технологій для захисту даних. Це передбачає впровадження криптографічних методів захисту, системи управління доступом, міжмережевих екранів, систем виявлення вторгнень, антивірусного захисту тощо. Основна перевага цього підходу полягає в його високій ефективності проти технічних загроз, таких як хакерські атаки або зловмисне програмне забезпечення [5, с. 50].

Правовий підхід охоплює створення та впровадження нормативно-правової бази, що регулює питання захисту інформаційних ресурсів держави. До таких нормативних актів належать закони про захист інформації, персональних даних, кібербезпеку, а також міжнародні угоди та конвенції, що регулюють питання інформаційної безпеки. Правове регулювання є невід'ємною частиною загального механізму забезпечення інформаційної безпеки, оскільки воно встановлює правила і норми для всіх суб'єктів інформаційних відносин [7, с. 105].

Організаційний підхід спрямований на побудову системи управління інформаційною безпекою на всіх рівнях державного управління. Він передбачає створення спеціалізованих державних органів, відповідальних за моніторинг та забезпечення безпеки інформаційних ресурсів, а також розробку стратегій і політик у сфері інформаційної безпеки. Важливу роль відіграють регулярні навчання та тренування персоналу, що забезпечують оперативне реагування на загрози [8, с. 140]. Необхідно зазначити, що інформаційна безпека держави стикається з численними загрозами, які можуть мати як внутрішній, так і зовнішній характер. До основних загроз можна віднести кібератаки, витоки інформації, шпигунство, саботаж інформаційних систем, дезінформацію та інформаційні війни. Кібератаки є однією з найсерйозніших загроз для державних інформаційних систем. Зокрема, мова йде про атаки на критичну інфраструктуру держави, що включає системи енергетики, транспорту, зв'язку, фінансів. Особливо небезпечними є кібератаки з використанням шкідливих програм типу «вимагачів» (ransomware) та DDoS-атаки [5, с. 55].

Витоки інформації можуть виникати як наслідок недостатньо захищених інформаційних систем або людського фактору. Ризики таких витоків особливо високі у випадку роботи з конфіденційними державними документами або персональними даними громадян. Порушення конфіденційності може призвести до значних втрат для держави та її громадян, зокрема до поширення чутливої інформації серед конкурентів або злочинних угруповань [6, с. 80].

Шпигунство та саботаж є ще однією серйозною загрозою для інформаційної безпеки держави. У сучасному глобалізованому світі шпигунські операції все частіше здійснюються через кіберпростір. Це може включати проникнення у державні бази даних, злам систем управління критичними об'єктами інфраструктури або саботаж інформаційних систем з метою їх пошкодження або виведення з ладу [7, с. 110].

Таблиця 1

Частота шпигунських кібератак за останні 5 років

Частота шпигунських кібератак за останні 5 років					
Рік	2019	2020	2021	2022	2023
Кількість	50	75	120	180	250

Для забезпечення інформаційної безпеки держави необхідно використовувати комплексний підхід, що включає технологічні, правові та організаційні заходи. Важливим аспектом є також міжнародна співпраця у сфері кібербезпеки, оскільки багато загроз мають транскордонний характер.

На технологічному рівні для захисту інформаційних ресурсів використовуються такі засоби, як міжмережеві екрани, системи виявлення вторгнень, антивірусні програми та криптографічні алгоритми шифрування даних. Однак, жодна технологія не може гарантувати абсолютної безпеки. Тому державам необхідно постійно оновлювати свої системи захисту, проводити тестування на проникнення (penetration testing) і регулярно переглядати свої стратегії безпеки [8, с. 145].

На правовому рівні важливо забезпечити створення комплексної нормативно-правової бази, що регулює всі аспекти захисту інформації та кібербезпеки. Закони повинні не тільки визначати права та обов'язки суб'єктів інформаційних відносин, але й передбачати відповідальність за порушення цих норм [9, с. 170].

На додаток, правові заходи включають створення ефективних механізмів правозастосування. У цьому контексті особливо важливим є підготовка відповідних органів, таких як національні агентства з кібербезпеки, правоохоронні органи та спецслужби, які можуть швидко реагувати на кіберінциденти. Також слід створювати міжнародні договори і співпрацювати з іншими країнами у сфері інформаційної безпеки, щоб спільно протидіяти загрозам, які виникають в цифровому середовищі [9, с. 172].

Організаційні механізми включають створення спеціалізованих структур державного рівня, відповідальних за забезпечення інформаційної безпеки. Наприклад, органи національної безпеки та оборони мають здійснювати постійний моніторинг стану інформаційної безпеки, розробляти стратегії запобігання та реагування на потенційні загрози. Такі організації повинні мати в своєму розпорядженні необхідні ресурси для швидкого та ефективного вирішення кризових ситуацій у сфері інформаційної безпеки [10, с. 195]. Інформаційна безпека також потребує інновацій, тому держава повинна інвестувати в дослідження і розробки у цій галузі, створювати стимулюючі програми для розвитку нових технологій і залучати до цього процесу приватний сектор [11, с. 220].

В умовах глобалізації інформаційного простору, окремі країни не можуть самостійно ефективно протидіяти кіберзагрозам. Спільні загрози, такі як кібертероризм, глобальні шпигунські мережі та міжнародна організована злочинність, вимагають координації зусиль на міжнародному рівні. Тому однією з ключових складових національної інформаційної безпеки є участь у міжнародних організаціях, таких як ООН, ЄС, НАТО та інших міждержавних структурах, що займаються питаннями кібербезпеки [12, с. 245].

Міжнародні ініціативи можуть включати спільні програми з навчання спеціалістів у сфері кібербезпеки, розвиток стандартів захисту інформації та впровадження передових технологій для боротьби з кіберзлочинністю. Крім того, важливо забезпечувати виконання міжнародних договорів у сфері кібербезпеки та створювати механізми для швидкого реагування на загрози глобального масштабу [13, с. 275]. Ефективне забезпечення інформаційної безпеки неможливе без розробки і впровадження державної політики у цій сфері. Державна політика повинна базуватися на принципах відповідальності, прозорості, системності та постійної адаптації до нових викликів. Важливо, щоб вона враховувала всі аспекти захисту інформації: від технічних і правових до організаційних та міжнародних. Основними елементами державної політики в сфері інформаційної безпеки повинні бути:

Створення комплексної нормативно-правової бази. Закони та інші нормативні акти мають чітко регулювати питання захисту інформації, передбачати відповідальність за її порушення і забезпечувати виконання вимог з боку як державних органів, так і приватних підприємств [7, с. 110].

Розробка національної стратегії інформаційної безпеки. Ця стратегія має враховувати наявні та потенційні загрози, визначати основні напрями роботи у сфері кіберзахисту та створювати механізми для їх реалізації [5, с. 48].

Підтримка наукових досліджень та інновацій. Держава повинна інвестувати в розвиток нових технологій для забезпечення інформаційної безпеки, стимулювати приватний сектор до участі у розробці засобів кіберзахисту [7, с. 220].

Навчання та підготовка спеціалістів. Для ефективного забезпечення інформаційної безпеки необхідно мати кваліфіковані кадри. Це передбачає регулярне підвищення кваліфікації працівників державних структур, проведення тренінгів та вебінарів [8, с. 145].

Підвищення обізнаності громадян. Інформаційна безпека стосується не лише держави, але й кожного громадянина. Тому важливо проводити інформаційні кампанії, що пояснюють населенню основні принципи кібербезпеки [6, с. 80].

Співпраця з приватним сектором. Держава повинна створювати умови для публічно-приватного партнерства, забезпечувати підтримку бізнесу у сфері кібербезпеки та заохочувати компанії до впровадження стандартів захисту інформації [9, с. 170].

Висновки і пропозиції. Проведене дослідження механізму забезпечення інформаційної безпеки держави дозволяє зробити такі висновки: інформаційна безпека держави є надзвичайно важливою складовою національної безпеки в умовах стрімкого розвитку інформаційного суспільства та глобалізації кіберпростору. Забезпечення інформаційної безпеки держави є одним з найактуальніших викликів сучасності, яке вимагає системного підходу, що включає технологічні, правові, організаційні заходи та міжнародне співробітництво. Державна політика в сфері інформаційної безпеки повинна базуватися на комплексному підході, що враховує як внутрішні, так і зовнішні загрози, а також забезпечує постійну адаптацію до нових викликів у цій сфері. Для цього необхідно розвивати нормативно-правову базу, підтримувати наукові дослідження, навчати спеціалістів, підвищувати обізнаність громадян та активно співпрацювати з приватним сектором і міжнародними партнерами. Лише за умови спільних зусиль держави, бізнесу та громадянського суспільства можна забезпечити стійкість інформаційного простору та захистити національні інтереси. Окрім того, міжнародне співробітництво є ключовим фактором забезпечення інформаційної безпеки, адже кіберзагрози мають транскордонний характер, тому співпраця між державами є необхідною для ефективного протистояння їм.

Тож, для ефективного забезпечення інформаційної безпеки держави потрібні спільні зусилля всіх учасників інформаційного простору, а також постійна модернізація засобів захисту відповідно до нових загроз і викликів сучасного цифрового світу. Ця стаття продемонструвала, що інформаційна безпека – це не статична концепція, а динамічний процес, який потребує постійної адаптації до нових умов. Інформаційна безпека є одним із пріоритетних напрямків державної політики. Від ефективності заходів з її забезпечення залежить стабільність суспільства, економічний розвиток і національна безпека.

ЛІТЕРАТУРА

1. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник.. К. : КНТ, 2006. 280 с.
2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України від 09 січня 2007 р. № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%E (дата звернення: 18.10.2024).

3. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
4. Конституція України від 28 червня 1996 р. URL: http://zakon5.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 18.10.2024).
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 18.10.2024).
6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 18.10.2024).
7. Волошин В. І. Інформаційна безпека держави: правові та організаційні аспекти. Київ: Науково-дослідний центр з питань інформаційної безпеки. 2020. 168 с.
8. Абрамов В. П. Основи кібербезпеки: сучасні виклики та механізми протидії. Харків: Юрінком Інтер. 2021. 298 с.
9. Кондратьєв С. О., Марченко, Л. П. Кібербезпека: міжнародні стандарти та національні механізми захисту. Дніпро: Вид-во ДНУ. 2020. 305 с.
10. Проблеми інформаційної безпеки в Україні: аналітична доповідь. Київ: НАН. 2021. 32 с.
11. Стратегія кібербезпеки України. Державна служба спеціального зв'язку та захисту інформації України. 2022. URL: www.dsszzi.gov.ua. (дата звернення: 18.10.2024).
12. Smith, J. Artificial Intelligence in Information Security. *Journal of Cybersecurity*. 2021. № 15(3). 234-250.
13. Brown, M. Cybersecurity Policies and Strategies. *International Journal of Information Security.* 2023. № 20(1). 275-290.