

*Р. В. Бондаренко,  
слухач магістратури кафедри управління охороною здоров'я та публічного адміністрування,  
Національний університет охорони здоров'я України імені П. А. Шупика*

*ORCID ID: 0000-0003-3581-0401*

*В. М. Михальчук,*

*д. мед. н., професор, завідувач кафедри управління охороною здоров'я та публічного  
адміністрування, Національний університет охорони здоров'я України імені П. А. Шупика,  
ORCID ID: 0000-0002-5398-4758*

DOI: 10.32702/2306-6814.2021.5.95

## ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

R. Bondarenko,

Master's student of the Department of Management health care and public administration,  
Shupyk National Healthcare University of Ukraine Kyiv, Ukraine

V. Mykhalchuk,

Doctor of Medical Sciences, Professor, Head of the Department of Healthcare Management  
and Public Administration, Shupyk National Healthcare University of Ukraine Kyiv, Ukraine

### INFORMATION SECURITY OF THE STATE

**У статті систематизовано теоретико-методологічні погляди науковців до розуміння категорії "інформаційна безпека держави" як важливого показника в контексті забезпечення національної безпеки в умовах глобалізації. Проблеми забезпечення ефективної інформаційної безпеки держави й суспільства, набувають великого значення у вітчизняній національній політиці та державному управлінні. Дослідження механізму розвитку інформаційної безпеки розглядається як важливе завдання захисту інформаційного простору в системі модернізації української державності та визначенні її ролі у світовій спільноті в період трансформації. В статті сформульовано трактування поняття "інформаційна безпека" як стан захищеного інформаційного простору, що здатен забезпечити реалізацію загальнонаціональних інтересів, збереження стійкості держави до екзогенних і ендемогенних чинників, що становлять загрозу та пов'язані із активним розвитком цифровізації. Узагальнення наукової бази дозволило виявити три концептуальні підходи до дослідження категорії "інформаційна безпека": 1) складова національної безпеки; 2) захищеність інформаційного простору та державних інтересів від можливих ризиків; 3) загальний показник стану системи захисту, що забезпечує основні критерії безпеки. Розглянуто чинники інформаційної безпеки в контексті розвитку інформаційного простору.**

**Доведено, що забезпечення інформаційної безпеки України є провідним напрямом державної політики, від якого залежить її національна безпека та соціально-економічний розвиток. Ефективний механізм захисту інформаційної безпеки України полягає в розробці відповідного правового законодавства врегулювання відносин, що виникають в інформаційній сфері та узгоджених діях суб'єктів на всіх рівнях забезпечення інформаційної безпеки України. Проаналізовано актуальні проблеми інформаційної безпеки, що перешкоджають сталому розвитку сфери інформаційно-комунікаційних технологій.**

**The article systematizes the theoretical and methodological views of scientists to understand the category of "information security of the state" as an important indicator in the national security in a globalization context. Problems of ensuring effective information security of the state and society are of great importance in domestic national policy and public administration. The study of the mechanism of information security development is considered to be a highly important task in**

*protecting the information space in the system of modernization of Ukrainian statehood and determining Ukraine's role in the world community in the transformation period. We involve general scientific, philosophical and special scientific methods in the methodological component of the study (systemic and institutional methods, synergetics, social dialectics, comparative analysis and synthesis, identification, etc.). The interpretation of the concept of "information security" is 'formulated' as a state of protected information space that can ensure the realization of national interests, maintaining the state's resilience to exogenous and endogenous factors that pose a threat and are associated with the active development of digitalization. The generalization of the scientific base allows identification of three conceptual approaches to the study of the category "information security": 1) The component of national security; 2) Protection of information space and state interests from possible risks; 3) The general indicator of a condition of system of protection providing the basic criteria of safety.*

*Factors of information security in the context of information space development are considered. Ensuring information security of Ukraine is the leading direction of state policy, on which its national security and socio-economic development depend. An effective mechanism for protecting the information security of Ukraine is to develop appropriate legal legislation to regulate relations arising in the information sphere and concerted actions of entities at all levels of information security of Ukraine. The current problems of information security that hinder the sustainable development of information and communication technologies need to be analysed as a priority.*

*Ключові слова: інформація, інформаційна безпека, національна безпека, система забезпечення інформаційної безпеки, загрози, державне управління.*

*Key words: Information, information security, National security, information security system, threats, public administration.*

## ПОСТАНОВКА ПРОБЛЕМИ

У кінці ХХ ст. інформація для будь-якої держави стає стратегічно важливим ресурсом, від ефективного використання якого залежить безпека країни та перспективи формування демократичного суспільства, де реалізуються всі конституційні права та свободи громадян, у тому числі право вільного пошуку, отримання, передачі та розповсюдження інформації усіма можливими законними засобами.

З розвитком засобів інформації суспільство мимоволі підключилось до глобальних інформаційних систем, стаючи суб'єктом даних систем. Соціальні умови життя населення в багатьох аспектах визначаються досконалістю інформаційних технологій. В політичній сфері все більше значення набувають не силові, а інформаційні чинники. В економіці відбувається інтеграція інформаційної продукції в систему товарних відносин. У результаті глобальної інформатизації відбувся якісний стрибок у процесах управління всіх рівнів.

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.

Інформаційна безпека є важливою невід'ємною складовою забезпечення національної безпеки держави. 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. 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. Зацікавленими у розвитку цього сектору є не тільки бізнес-структури, що активно застосовують нововведення у даній сфері, а й державні установи, для яких найголовнішим є питання національної безпеки. Отже, потреба забезпечення національної безпеки належить до концептуальних основ діяльності суспільства. Усе це й зумовлює необхідність ґрунтовного дослідження категорії "інформаційна безпека держави".

## АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Вирішенню проблеми встановлення сутності поняття "інформаційна безпека" присвячені чисельні роботи як вітчизняних, так і закордонних науковців. Серед зарубіжних вчених вагомий внесок у дослідження питання інформаційної безпеки внесли: П. Друкер, Г. Кіссінджер, К. Мак-Коннел, Ч. Флавін. Серед сучасних вітчизняних дослідників хотілося б відзначити праці: О.В. Адамчука, Г.А. Атаманова, О.І. Барановського, А.Ю. Берко, О.В. Глазової, В.М. Грубова, В.В. Домарьова, В.Б. Дудикевича, В.В. Карасюка, О.О. Левіна, О.С. Олексюка, І.В. Рішняк, М.А. Судейко, І.О. Трубіна тощо. Однак попри вагомий внесок даних учених, враховуючи постійний вплив зовнішніх та внутрішніх чинників, доцільним є детальніший розгляд питань розвитку інформаційної безпеки як пріоритетного складника національної безпеки України.

## МЕТА СТАТТІ

Метою статті є систематизація сучасних наукових підходів до розкриття сутності поняття "інформаційна

безпеку держави" на основі детального аналізу представлених у науковій літературі понять.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Наслідком швидкого розвитку інформаційно-комунікаційних технологій є зміна наукових картин світу та суттєва трансформація життя суспільства. Інформація усвідомлюється як важливий економічний ресурс. Ефективна організація інформаційних процесів істотно збільшить рентабельність багатьох видів діяльності, сприятиме вирішенню політичних та соціально-економічних проблем. Нині всесвіт опинився перед новими викликами у сфері забезпечення інформаційної безпеки. В сучасних умовах глобалізації інформаційна безпека виступає одним з найголовніших чинників забезпечення умов реалізації національних інтересів, спроможності держави долати кризові явища під час зовнішньої агресії. Особливо гостро це питання привертає увагу до тих процесів, що відбуваються в Україні в умовах гібридної війни та окупації частини української території.

Своєчасні ефективні заходи з управління інформаційною безпекою з боку держави, як основного суб'єкта забезпечення інформаційної безпеки, здатні подолати загрози соціально-економічному та політичному життю країни.

Перед тим як детальніше розглянути зміст категорії "інформаційна безпека держави" доцільним буде розкрити сутність поняття "інформація" та "національна безпека".

Починаючи з XX ст. слово "інформація" почало застосовуватись у наукових галузях та отримало певні тлумачення. Сучасній науці відомо два основних концептуальні визначення інформації:

- інформація є невід'ємною внутрішньою властивістю кожного матеріального об'єкта;
- інформація нерозривно пов'язана з функціонуванням та управлінням.

Відзначимо, що першим, дослідником інформатики як науки був Н. Вінер, він розглядав інформацію як позначення змісту, отриманого з зовнішнього світу в процесі нашого пристосування до нього і пристосування наших почуттів. Інформація є інформація, а не матерія і не енергія. Він стверджував, що процес отримання та використання інформації є процесом нашого пристосування до випадковостей зовнішнього середовища і нашої життєдіяльності в цьому середовищі [3, с. 17].

Український вчений В.М. Глушков зазначає, як фізична субстанція інформація являє собою міру неоднорідності розподілу матерії та енергії в просторі та в часі, міру змін, якими супроводжуються всі процеси, що протікають у світі [4, с. 32].

Згідно із Законом України "Про інформацію", інформація — будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [12]. Науково-технічна інформація — будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [12].

Категорію "національна безпека", яка є ключовою дослідники визначають, з одного боку, "поняття "національна безпека" стало невід'ємним атрибутом більшості воєнно-політичних концепцій, аналітичних та прогностичних розробок довгострокового, глобального характеру". З іншого боку, "й досі немає чіткої, загальновизнаної дефініції поняття "національна безпека", і до того ж "розбіжності між науковими школами та окремими дослідниками досить радикальні" [1, с. 13].

Останнім часом методологічні підходи до визначення ключових понять і категорій основ національної безпеки передбачають, щоб "під національною безпекою... розуміти необхідний і динамічний стан відносної невразливості держави, який визначає характер взаємодії з зовнішнім середовищем і забезпечується переважно спільними зусиллями зовнішньополітичних, силових і координаційних державних органів у спосіб використання різних засобів в умовах явного чи прихованого, прямого чи опосередкованого негативного впливу внутрішніх чинників на прийняття рішень у сфері забезпечення життєдіяльності і розвитку держави, а також системи забезпечення її безпеки" [15, с. 15].

Національна безпека — це категорія, яка характеризує ступінь захищеності життєво важливих інтересів, прав та свобод особи, суспільства і держави від зовнішніх і внутрішніх загроз або ступінь відсутності загроз правам і свободам людини, базовим інтересам і цінностям суспільства та держави [5, с. 45].

Під загрозою розуміється можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого, те, що може заподіяти зло чи неприємність [2, с. 387].

Загрози національній безпеці України — явища, тенденції і чинники, що унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [14, с. 27].

Інформаційній безпеці сьогодні приділяється значна увага як науковців, так і держави. Нині у науковій літературі склалося три основні концептуальні підходи до визначення сутності інформаційної безпеки:

- інформаційна безпека як складова національної безпеки;
- інформаційна безпека як стан захищеності інформаційного середовища та національних інтересів від можливих загроз;
- інформаційна безпека як стан системи, який здатний забезпечити цільові параметри безпеки.

Під інформаційною безпекою розуміють якість захищеності об'єкта, яким найчастіше виступає інформація, дані та ресурси системи. Безпека інформації — це стан захищеності даних, що забезпечує їх доступність, конфіденційність та цілісність.

На думку В.С. Цимбалюк, А.В. Бабінської, під інформаційною безпекою України слід розуміти стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства та держави [14, с. 23]. О.А. Нішменко вважає, що інформаційна безпека це стан захищеності національних інтересів України в інформаційній сфері, що складаються з сукупності збалансованих інтересів особи, суспільства та держави від внутрішніх і

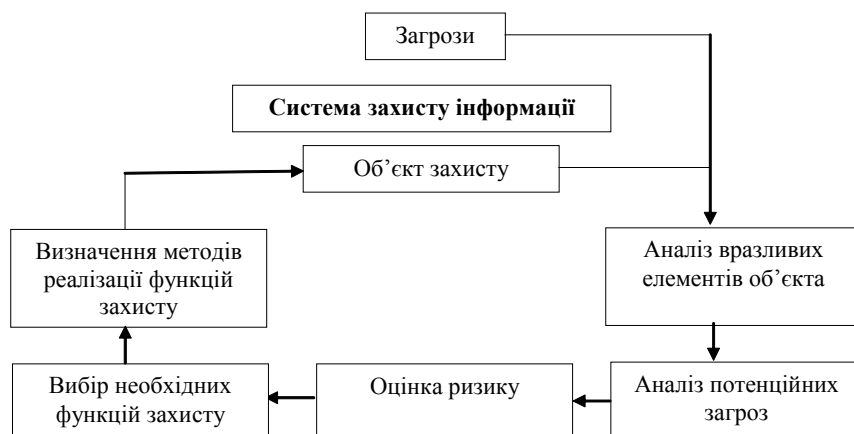


Рис. 1. Система захисту об'єкта

зовнішніх загроз, що відповідає принципу забезпечення національної безпеки в інформаційній сфері [10, с. 19]. На думку Л.О. Кочубей, інформаційна безпека — це такий стан захищеності життєво важливих інтересів, а отже, й інформаційної озброєності держави, суспільства, особистості, за якого жодні інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів — [8, с. 221—222]. За визначенням В.В. Шемчука, інформаційна безпека — це правовідносини, що виникають під час здійснення превентивних і захисних заходів в інформаційному середовищі людини, суспільства та держави [10, с. 23].

Інформаційна безпека це стан захищеності особи, суспільства, держави від інформації, що носить шкідливий або протиправний характер та від інформації, що чинить негативний вплив на свідомість особистості, перешкоджає сталому розвитку особи, суспільства й держави. Інформаційна безпека забезпечує сталий розвиток особи, суспільства, держави та захищає інформаційну інфраструктуру (комп'ютери, інформаційно-телекомунікаційну інфраструктуру).

Проблема забезпечення безпеки інформації не є новою. Впродовж багатьох років суспільство вирішує завдання зі створення засобів та систем зберігання, обробки, передачі та захисту інформації. На рисунку 1 зображено загальну концепцію побудови систем захисту інформації. Дана концепція має забезпечити єдність принципів формування та проведення заходів державного управління на всіх етапах системи захисту інформаційної сфери.

Забезпечення інформаційної безпеки здійснюється на основі поєднання законодавчої, правоохоронної, судової, контрольної та інших форм діяльності державних органів у взаємодії з органами місцевого самоуправління, організаціями та громадянами.

Основний вектор державного управління у сфері інформаційної безпеки спрямований на виявлення та нейтралізацію існуючих ризиків інформаційної безпеки з врахуванням усіх чинників, що мають вплив як на державні структури так і на інформаційні системи.

Менеджмент інформаційної безпеки включає в себе декілька рівнів:

1) рівень міжнародних професійних об'єднань, що пов'язані зі сферою інформаційних технологій, телекомунікацій та інформаційної безпеки;

2) рівень крупних компаній, працюючих у сфері інформаційних технологій, що у значній мірі визначають стан інформаційної безпеки у суспільстві користувачів інформаційних систем, а також мають вплив на безпеку різних елементів інформаційної інфраструктури;

3) державний рівень — рівень державних організацій, що впливають на життя суспільства, стан правової системи, розвиток економіки та технологій;

4) рівень окремих компаній — спільнота користувачів інформаційних систем, що зацікавлені у власній інформаційній безпеці та забезпечують захист наявних інформаційних ресурсів власними силами.

Для кожного рівня вказаної ієрархії характерні свої завдання та специфічні методи організаційної роботи.

Діяльність держави в галузі інформаційної безпеки, як правило, будується, на загальних завданнях державної влади, зокрема:

- збереження принципу суверенітету держави;
- політична стабільність;
- розвиток демократичних інститутів суспільства, а також забезпечення прав і свобод громадян;
- укріплення законності та правопорядку;
- соціально-економічний розвиток країни та стійкість фінансової системи.

Проблеми інформаційної безпеки можна розділити на три великих групи:

— проблеми гуманітарного характеру — проблеми інформаційної безпеки, що виникають у зв'язку з неконтрольованим використанням та розповсюдженням персональних даних громадян та вторгненнями у приватне життя;

— проблеми економічного та юридичного характеру — виникають у результаті загубленої чи вкраденої комерційної та фінансової інформації;

— проблеми політичного характеру — проблеми інформаційної безпеки, що виникають внаслідок інформаційної війни, кібервійни та електронної розвідки в інтересах політичних угруповань, компрометація державної таємниці, атаки на інформаційні системи важливих оборонних, транспортних та промислових об'єктів.

Механізм забезпечення інформаційної безпеки держави реалізується через застосування органами



Таблиця 1. Чинники інформаційної безпеки держави

№ з/п	Чинник	Характеристика
1	Соціально-економічний чинник	Формує економічне підґрунтя інформаційного розвитку держави й суспільства та матеріально-технічні можливості впровадження інформаційно-комунікаційних технологій. Узагальнені соціально-економічні чинники (стабільний розвиток економіки, високий рівень забезпеченості населення та апарату держави необхідними для розвитку матеріально-технічними та інформаційно-комунікаційними засобами, достатній рівень фінансування сфери освіти та науки) визначають результативність процесу забезпечення інформаційної безпеки
2	Правовий чинник	Створення досконалого інформаційного законодавства, що регламентує інформаційну сферу суспільних відносин та його ефективну реалізацію (вдосконалення нормативної бази з протидії комп'ютерній злочинності, захист інформації з персональних даних і державної таємниці, підвищення рівня правової свідомості громадян в інформаційно-комунікаційній сфері)
3	Технологічний чинник	Сукупність організаційно-технічних та спеціальних засобів, що формують технічну досконалість і сучасність засобів обробки інформації та спрямовані на ефективне функціонування інформаційної сфери (розвинена мережа швидкісного Інтернету, досконалість інформаційних ресурсів; новітні автоматизовані системи обробки та передачі інформації)

Джерело: побудовано за [6, с. 125].

виконавчої влади таких адміністративно-правових засобів:

1) дозвільних засобів, що включають дозвіл на провадження діяльності, пов'язаної з державною таємницею, стандартизацію заходів забезпечення інформаційної безпеки, ліцензування та легалізацію;

2) реєстраційних засобів, які включають реєстрацію засобів масової інформації та державну реєстрацію персональних баз даних;

3) засобів адміністративно-правового примусу, до яких слід, насамперед, віднести засоби адміністративної відповідальності.

У контексті інформаційного розвитку суспільства та забезпечення інформаційної безпеки можна виділити наступні чинники (табл. 1).

У ст. 17 Конституції України закріплено, що захист суверенітету та територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є най-

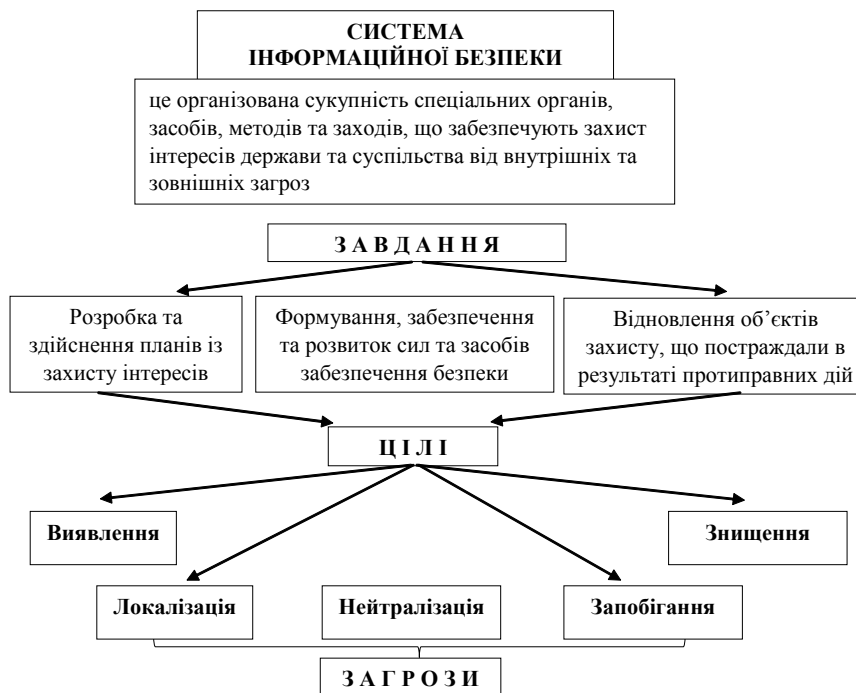


Рис. 2. Система інформаційної безпеки держави

важливішими функціями держави, справою всього Українського народу [7]. Отже, інформаційну безпеку потрібно розглядати, як ефективну протидію зовнішнім та внутрішнім загрозам з метою забезпечення інформаційного суверенітету. Водночас під інформаційним суверенітетом держави на законодавчому рівні розуміється здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави [13].

Інформаційна безпека розглядається поряд з кібербезпекою, захистом персональних даних, недоторканістю особистого життя та прав користувачів цифрових технологій, зміцненням та захистом довіри у кіберпросторі визначається передумовою одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками.

Також інформаційна безпека розкривається у Доктрині інформаційної безпеки України від 25 лютого 2017 р. [11] як невід'ємна складова кожної зі сфер національної безпеки і як важлива самостійна сфера забезпечення національної безпеки.

Забезпечення інформаційної безпеки є невід'ємним процесом реалізації системи національної безпеки (рис. 2).

Основними функціями системи забезпечення інформаційної безпеки є:

- попереджувальна: здійснення комплексу заходів, спрямованих на попередження та нейтралізацію загроз;
- прогностична: прогнозування та ідентифікація внутрішніх і зовнішніх загроз;
- управлінська: створення умов та можливостей для ефективного управління інформаційними ресурсами.

Інформаційна безпека держави багато в чому залежить від загального фінансово-економічного стану та політики, що проводиться в державі.

Серед завдань, які повинні виконувати суб'єкти системи забезпечення інформаційної безпеки слід виділити такі:

- виявлення чинників, ризиків і загроз інформаційній безпеці;
- визначення індикаторів інформаційної безпеки і порівняння їх з граничною межею;
- розробка системи моніторингу, що включатиме спостереження, збирання, обробку, зберігання і аналіз інформації щодо стану інформаційної безпеки держави;
- розробка заходів, спрямованих на зміцнення інформаційної безпеки держави.

Узагальнюючи підходи до розкриття змісту категорії "інформаційна безпека держави", можна визначити основні її особливості:

- 1) є складовою національної безпеки та швидко розвивається як в Україні, так і в світі, глобальна інформатизація охоплює всі сфери держави;
- 2) це стан захисту об'єкта, за якого досягається його ефективна діяльність незалежно від ендегенних і екзогенних інформаційних впливів;
- 3) це стан її захищеності, за якого сучасні інформаційні акти агресії не завдають шкоди національним інтересам.

У сучасних умовах інформаційна сфера вимагає прийняття адекватних заходів протидії ескалації іноземного інформаційного впливу в усіх його проявах. Шляхи вирішення даної проблеми полягають в наступних напрямках:

- систематичній діяльності з запобігання загрозам інформаційному простору, структуризація цілей та завдань з питань забезпечення інформаційної безпеки в фінансово-економічній сфері;
- активній протидії впливу на свідомість населення з метою зміни національних ідеологічних установок;
- розвитку вітчизняної технологічної та виробничої бази в галузі інформаційних технологій;
- підвищенні безпеки інформаційно-телекомунікаційних систем в сфері інформатизації озброєння та військової техніки;
- охорони державної таємниці, а також — іншої інформації з обмеженим доступом;
- вдосконаленні структури забезпечення інформаційної безпеки у сфері оборони [9, с. 744];
- захисті вітчизняного інформаційного простору від розповсюдження забороненої інформаційної продукції;
- обміні досвідом в інформаційно-комунікаційній галузі, а також підготовці кваліфікованих фахівців відповідно до вищих професійних стандартів.

## ВИСНОВКИ

Захист інформації — гарантія безпеки та одне з першочергових завдань держави. Активний розвиток в рамках постіндустріального суспільства призводить до того, що інформація стає повноцінним ресурсом на одному рівні з економічними, фінансовими та виробничими ресурсами. Від правильно побудованої системи державного управління безпекою залежить стан захисту інформаційного простору, що здатен забезпечити реалізацію загальнонаціональних інтересів, збереження стійкості держави до внутрішніх й зовнішніх негативних чинників, що становлять загрозу та пов'язані із активним розвитком цифровізації.

Забезпечення інформаційної безпеки перетворилось в актуальну глобальну проблему нашого часу. Цей процес варто розглядати на одному рівні з проблемами збереження та розвитку культури, припинення війни та озброєних конфліктів, забезпечення економічної, екологічної, демографічної та енергетичної безпеки. Основними завданнями ефективної діяльності у сфері державного управління інформаційною безпекою є:

- розробка критеріїв та методів оцінки ефективності систем захисту інформаційної безпеки держави;
- ідентифікація та попередження появи дестабілізуючих чинників та інформаційних загроз, проведення їх моніторингу;
- організація проведення фундаментальних та прикладних наукових досліджень в галузі забезпечення інформаційної безпеки;
- розробка та прийняття відповідних нормативно-правових актів;
- впровадження єдиної системи ліцензування та сертифікації в даній сфері;
- протистояння загрозі інформаційної війни.

Особливістю розвитку в сфері захисту інформаційного простору України є те, що її система знаходиться

на етапі свого становлення. Відсутня чітка та узгоджена концепція забезпечення інформаційної безпеки, наслідком цього є негативний вплив на інформаційний простір, що ставить під загрозу інформаційну незалежність держави.

#### Література:

1. Бодрук О.С. (2001). Структури воєнної безпеки: національний та міжнародний аспекти: монографія. Київ: НІПМБ. 300.

2. Бусел В.Т. (2007). Великий тлумачний словник сучасної української мови. Київ: ВТФ "Перун". 1736.

3. Вiner, N. (1983). Кибнетика, или управление и связь в животном и машине. Москва: Наука. 344.

4. Глушков В.М. (1964). Про кибернетику как наука. Кибернетика, мышление, жизнь. Москва: Мысль. 511.

5. Гончаренко О., Джангужин Р., Лисицин Е. (2003). Громадянський контроль і система національної безпеки. Національна безпека України. № 1. 39—46.

6. Кавун С.В. (2008). Інформаційна безпека: навчальний посібник. Харків: Харківський національний економічний ун-т. 196.

7. Конституція України [Електронний ресурс]: Прийнята Верховною Радою України 28.06.1996. — Режим доступу: <http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/ed19960628>

8. Кочубей Л.О. (2015). Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса. Вип. 3. 220—237.

9. Кравець Є.А. (1992). Інформаційна безпека держави. Київ: Укр. енцикл. 1235.

10. Ніщименко О.А. (2016). Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. № 1. 17—23.

11. Про Доктрину інформаційної безпеки України [Електронний ресурс]: Указ Президента України від 25.02.2017 № 47/2017. Режим доступу: <https://www.president.gov.ua/documents/472017-21374>

12. Про інформацію [Електронний ресурс]: Закон України № 2657-XII від 02.10.1992. — Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

13. Про Національну програму інформатизації [Електронний ресурс]: Закон України № 74/98-ВР від 04.02.1998. Режим доступу: <https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text>

14. Цимбалюк В.С., Бабінська А.В. (2014). Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. Адміністративне право і процес. № 2 (8). 22—30. URL: <http://aplaw.net/index.php/journal/issue/view/18/4-8-2014-pdf>

15. Шипілова Л.М. (2007). Порівняльний аналіз ключових понять і категорій основ національної безпеки України: автореф. дис. к. політ. н.: 21.01.01. Київ. 20.

#### References:

1. Bodruk, O.S. (2001), *Struktury voiennoi bezpeky: natsionalnyj ta mizhnarodnyj aspekty: Monohrafiia* [The Structure of Military Security and International Aspects: Monograph], NIPMB, Kyiv, Ukraine.

2. Busel, V.T. (2007), *Velykyj tлумachnyj slovnyk suchasnoi ukrainskoi movy* [The Big Explanatory Dictionary of Modern Ukrainian Language], VTF "Perun", Kyiv, Ukraine.

3. Viner, N. (1983), *Kibernetika, ili upravlenie i svyaz v zhivotnom i mashine* [Cybernetics: or the Control and Communication in the Animal and the Machine], 2nd ed, Nauka, Moscow, Russia.

4. Glushkov, V.M. (1964), *Pro kibernetiku kak nauka. Kibernetika, myshlenie, zhizn* [About Cybernetics as a Science. Cybernetics, Thinking, Life], Myisl, Moscow, Russia.

5. Honcharenko, O. Dzhanhuzhyn, R. and Lysytsyn, E. (2003), "Civil control and the National security system", *Natsionalna bezpeka Ukrainy*, vol. 1, pp. 39—46.

6. Kavun, S.V. (2008), *Informatsijna bezpeka* [The Information Security], *Kharkivskyj natsionalnyj ekonomichnyj un-t*, Kharkiv, Ukraine.

7. The Verkhovna Rada of Ukraine (1996), "The Constitution of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (Accessed 4 November 2020).

8. Kochubei, L.O. (2015), "Information security of state: defenses Ukrainian information field (for example, features information and communication technologies in modern Donbass)", *Naukovi zapysky Instytutu politychnykh i etnonatsionalnykh doslidzhen imeni I. F. Kurasa*, vol. 3, pp. 220—237.

9. Kravets, Ye.A. (1992), *Informatsijna bezpeka derzhavy* [The State Information Security], *Ukr. entsykl.*, Kyiv, Ukraine.

10. Nischymenko, O.A. (2016), "Information security of Ukraine at the present development of the state and society", *Nashe pravo*, vol. 1, pp. 17—23.

11. The Verkhovna Rada of Ukraine (2017), "The Doctrine of information security of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (Accessed 6 November 2020).

12. The Verkhovna Rada of Ukraine (1992), *The Law of Ukraine "About information"*, available at: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (Accessed 4 November 2020).

13. The Verkhovna Rada of Ukraine (1992), *The Law of Ukraine "About the National Informatization Program"*, available at: <https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text> (Accessed 5 November 2020).

14. Tsymbaliuk, V.S. and Babinska, A.V. (2014), "Legal regulation of information security in Ukraine: problems of theory and practice", *Administrativne pravo i protses*, [Online], vol. 2 (8), available at: <http://aplaw.knu.ua/index.php/arkhiv-nomeriv/2-8-2014/item/284-pravove-rehulyuvannya-informatsiynoyi-bezpeky-v-ukrayini-problemy-teoriyi-ta-praktyky-tsymbaliuk-v-s-baby> (Accessed 5 November 2020).

15. Shypilova, L.M. (2007), "The Comparative Analyses of the Key Concepts and Categories of the Ukraine's National Security Fundamentals", Ph.D. Thesis, *Fundamentals of national security (political science)*, Institute of National Security Problems under National Security and Defense Council of Ukraine, Kyiv, Ukraine. *Стаття надійшла до редакції 01.03.2021 р.*