УДК 351:342.57

В. В. Кушніков,
аспірант, Національний аерокосмічний університет "Харківський авіаційний інститут"
ORCID ID: https://orcid.org/ 0009-0003-0843-4516

DOI: 10.32702/2306-6814.2026.3.416

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

V. Kushnikov,
PhD student, National Aerospace University "Kharkiv Aviation Institute"

STATE POLICY IN THE FIELD OF ENSURING OF INFORMATION SECURITY IN THE CONTEXT OF HYBRID THREATS

У статті здійснено дослідження специфіки формування та реалізації державної політики у сфері забезпечення інформаційної безпеки в умовах гібридних загроз. Зокрема, визначено роль і місце інформаційної безпеки в державні політиці; обгрунтовано необхідність формування комплексної системи для вирішення проблем забезпечення інформаційної безпеки суспільства і держави; окреслено необхідні соціальні заходи, необхідні для забезпечення інформаційної безпеки на мікро-, мезо- та макрорівнях.

Зазначено, що весь спектр інтересів суб'єктів, пов'язаних з використанням інформаційно-комунікаційних технологій, можна поділити на такі категорії: забезпечення доступності, цілісності й конфіденційності інформації та підтримуючої інфраструктури.

Підкреслено, що за основними сферами прояву системне вираження інформаційної безпеки локалізується: у сфері функціонування органів державного управління (державна інформаційна безпека); у сфері громадянського суспільства (інформаційна безпека суспільства); у сфері інтересів особистості.

Визначено, що інформаційна безпека суспільства і держави характеризується ступенем їх захищеності основних сфер життєдіяльності (економіки, науки, техносфери, сфери державного управління тощо) відносно небезпечних, дестабілізуючих і деструктивних інформаційних впливів, що зачіпають інтереси країни на рівні як впровадження, так і вилучення інформації.

Відзначено, що в рамках державної політики на макрорівні соціальних заходів забезпечення інформаційної безпеки необхідно вжити наступних кроків: розробити узгоджену концепцію правового забезпечення інформаційної безпеки; запровадити практику популяризації основних принципів інформаційної безпеки, прав та обов'язків в інформаційній сфері; створити науково-методологічну базу у галузі інформаційної безпеки.

Констатовано, що максимальний ефект від зусиль, що докладаються на даному ступені популяризації знань з галузі інформаційної безпеки та інформаційної етики, може виражатися у збільшенні кількості соціальних суб'єктів, які набудуть здатності здійснювати попередні оцінки поведінки суб'єктів щодо ідентифікації соціальних та етичних проблем, що виникають.

The article studies the specifics of formation and implementation of the state policy in the field of ensuring of information security in the context of hybrid threats. In particular, the role and place of information security in the state policy are determined; the need to form a comprehensive system to solve the problems of ensuring of information security of society and the state is substantiated; the necessary social measures necessary to ensure information security at the micro, meso and macro levels are outlined.

It is noted that the entire spectrum of interests of entities related to the use of information and communication technologies can be divided into the following categories: ensuring of the availability, integrity and confidentiality of information and supporting infrastructure.

It is emphasized that according to the main areas of manifestation, the systemic expression of information security is localized: in the sphere of functioning of state administration bodies (state information security); in the sphere of civil society (information security of society); in the sphere of individual interests.

It is determined that the information security of society and the state is characterized by the degree of protection of the main spheres of life (economy, science, technosphere, public administration, etc.) concerning dangerous, destabilizing and destructive information influences that affect the country's interests at the level of both the introduction and extraction of information.

It is noted that within the framework of state policy at the macro level of social measures concerning ensuring of information security, the following steps must be taken: developing of a coordinated concept of legal support of information security; introducing of the practice of popularizing the basic principles of information security, rights and obligations in the information sphere; creating of a scientific and methodological base in the field of information security.

It is established that the maximum effect of the efforts made at this stage of popularization of knowledge in the field of information security and information ethics can be expressed in an increase of the number of social actors, who will acquire the ability to make preliminary assessments of the behavior of subjects in order to identify emerging social and ethical problems.

Ключові слова: державна політика, інформаційна безпека, гібридні загрози, інформаційна етика, комплексна система.

Key words: state polic, information security, hybrid threats, information ethics, complex system.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сьогодні інформаційна безпека постає як важлива та необхідна умова безпечного існування всієї світової спільноти. Основною особливістю її змісту стає закономірна тенденція зростання значення гуманістичної спрямованості, яка насамперед дозволить нейтралізувати основні небезпеки та загрози інформаційного характеру, забезпечуючи безпечне використання інформаційних технологій у суспільстві.

У даному контексті особливої значущості набуває оцінка інформаційно-технічних винаходів та перспектив використання інформаційних технологій, що впливають на виживання суспільства. Можливість мати достовірну інформацію про наслідки застосування інформаційних технологій сприяє попередженню негативних проявів різного характеру. Неповна чи недостовірна інформація, незнання чи нерозуміння наслідків є глибинною причиною основної кількості катастроф та аварій у майбутньому. Інакше гіпотетичне майбутнє людства має бути визначальним орієнтиром розвитку можливих напрямів системи інформаційних технологій. Від цього усунення пріоритетів у змісті інформаційної безпеки сьогодні неминуче вносить зміни до структури функціонування глобальної безпеки на підтримку загальнолюдських інтересів. Вищезазначене обумовлює актуальність обраної теми дослідження.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Аналіз публікацій щодо показує, що інформаційні технології, котрі використовуються суспільством, повинні отримувати соціальний зміст. Розробка та впровадження нових інформаційних технологій, що мають соціально-гуманістичну спрямованість, визначаються не тільки стараннями творців технологій, але, насамперед

суспільства, що формує сприятливе гуманістично спрямоване соціальне середовище. Це підтверджується точками зору багатьох вчених і практиків, зокрема, таких, як: Н.Г. Клименко, Г.П. Ситник, В.О. Торічний тощо. Проте недостатньо уваги приділяється розвитку державної політки у сфері інформаційної безпеки в умовах гібридних загроз.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою роботи є дослідження специфіки формування та реалізації державної політики у сфері забезпечення інформаційної безпеки в умовах гібридних загроз.

Для досягнення поставленої мети в роботі пропонується поставити та вирішити такі завдання:

— визначити роль і місце інформаційної безпеки в державні політиці;

— обгрунтувати необхідність формування комплексної системи для вирішення проблем забезпечення інформаційної безпеки суспільства і держави;

— окреслити необхідні соціальні заходи, необхідні для забезпечення інформаційної безпеки на мікро-, мезо- та макрорівнях.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Інформаційна сфера як сукупність інформації, засобів її продукування, обробки і зберігання, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, поширення й використання інформації, а також системи регулювання виникаючих при цьому суспільних відносин, будучи важливим фактором життя суспільства, активно впливають на стан державно-управлінської, економічної, оборонної та інших складових безпеки держав. Відтак, національна безпека держав у сучасному світі істотно залежить від забезпечення інформаційної безпеки, що дозволяє припустити, що з розвитком технічного прогресу ця залежність буде тільки зростати [1; 5].

Так, під інформаційною безпекою, як правило, розуміють захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації та інфраструктурі, що її підтримує.

Захист інформації — це комплекс заходів, спрямованих на забезпечення інформаційної безпеки. На нашу думку, адекватний з методологічної точки зору підхід до проблем інформаційної безпеки має починатися з виявлення суб'єктів інформаційних відносин та їх інтересів, пов'язаних з використанням інформаційно-комунікаційних технологій. Загрози інформаційній безпеці — це зворотний бік використання інформаційно-комунікаційних технологій.

Трактування проблем, пов'язаних з інформаційною безпекою різних категорій суб'єктів державного управління, може мати суттєві відмінності. Весь спектр інтересів суб'єктів, пов'язаних з використанням інформаційно-комунікаційних технологій, можна поділити на такі категорії: забезпечення доступності, цілісності й конфіденційності інформації та підтримуючої інфраструктури. Мета заходів у сфері інформаційної безпеки — захистити інтереси суб'єктів інформаційних відносин [2; 4].

Інтереси ці різноманітні, але всі вони згруповані навколо трьох основних аспектів: доступність, цілісність і конфіденційність. У цьому контексті інформаційну безпеку можна трактувати і як відсутність неприпустимого ризику, пов'язаного із заподіянням прямої або непрямої (в тому числі майнової, фінансової) шкоди підприємству (фізичній особі), що спричинено порушенням конфіденційності, цілісності й доступності інформації.

За основними сферами прояву системне вираження інформаційної безпеки локалізується:

— у сфері функціонування органів державного управління (державна інформаційна безпека);

— у сфері громадянського суспільства (інформаційна безпека суспільства);

— у сфері інтересів особистості [2; 3].

Говорячи про зміст і структуру інформаційної безпеки, слід враховувати, що категорія "інформаційна безпека" на даному етапі може мати різний зміст при використанні в різних контекстах. Так, в органах державного управління склалися дві тенденції при визначенні поняття та структури інформаційної безпеки. Представники так званого гуманітарного напрямку пов'язують інформаційну безпеку тільки з інститутом державної таємниці. У свою чергу представники силових структур пропонують поширити сферу інформаційної безпеки практично на всі питання і відносини в інформаційній сфері, фактично ототожнюючи інформаційну безпеку з інформаційною сферою. На наш погляд, обидві точки зору представляють крайні позиції.

Інтереси особистості в інформаційній сфері полягають у реалізації конституційних прав людини і громадянина на доступ до інформації, використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку. Інтереси суспільства в інформаційній сфері полягають у забезпеченні інтересів особистості в цій сфері, зміцненні демократії, створенні правової соціальної держави в Україні. Інтереси держави в інформаційній сфері визначаються створенням умов для гармонійного розвитку вітчизняної інформаційної інфраструктури, реалізації конституційних прав і свобод людини і громадянина у сірі отримання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності держави, політичної, економічної, державно-управлінської й соціальної стабільності, в безумовному забезпеченні законності та правопорядку, розвитку рівноправного й взаємовигідного міжнародного співробітництва [1; 4].

Інформаційна безпека суспільства і держави характеризується ступенем їх захищеності, а відтак — стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери державного управління і т.д.)

відносно небезпечних, дестабілізуючих і деструктивних інформаційних впливів, що зачіпають інтереси країни на рівні як впровадження, так і вилучення інформації. На нашу думку, інформаційна безпека в даному випадку визначається здатністю нейтралізувати такі впливи. Об'єктами небезпечного інформаційного впливу та, отже, інформаційної безпеки можуть бути: свідомість, психіка людей; інформаційно-технічні системи різного масштабу і призначення. Якщо говорити про соціальні об'єкти інформаційної безпеки, то до них можна віднести особистість, колектив, суспільство і державу [1; 5].

У рамках завдання захисту основних прав та фундаментальних свобод людини забезпечення максимального розмаїття легітимного контенту в інформаційних мережах передбачає задоволення насамперед тих інформаційних потреб, які сприяють прогресу людства. При цьому у питанні про раціональну інформаційну технологію, запрограмовану на повагу до людських цінностей, мається на увазі, що оволодіння суспільством знанням та інформацією за допомогою технологічних засобів буде спрямоване лише на прогресивний розвиток.

У свою чергу, виконання другої умови, що полягає у забезпеченні загального доступу до інформації та інформаційних технологій, передбачає розширення масштабу соціальної бази інформаційної безпеки, що призведе до поглиблення державного, громадського та особистісного рівнів функціонування. Громадянське суспільство, беручи зобов'язання щодо забезпечення всіх категорій свого населення рівними можливостями, у тому числі й участі в інформаційній взаємодії, без сумнівів, зацікавлене у розширенні масштабів соціальної бази інформаційної безпеки [2; 4].

Насправді процес зростання соціальної бази передбачає паралельне збільшення кількості суб'єктів інформаційної безпеки. У результаті проявляється важливе завдання, що полягає у підвищенні рівня освіти та інформаційної культури соціальних суб'єктів та суспільства загалом. Це питання охоплює як професійну діяльність у сфері інформаційних технологій, і рівною мірою будь-яку діяльність у інформаційному середовищі, що об'єднує всіх суб'єктів інформаційних відносин, оскільки саме рівень розвитку людських ресурсів як основна передумова формування наукового, соціального, економічного, культурного та духовного потенціалу зрештою визначає безпеку соціуму. У світлі зазначених перспектив наука та освіта виступають вирішальними факторами забезпечення інформаційної безпеки як основної складової національної безпеки [3; 5].

Тенденція зростання значення соціальної складової інформаційної безпеки веде до розуміння необхідності запровадження якісно нової форми захисту — соціальних заходів забезпечення інформаційної безпеки. Особлива новизна подібної форми захисту зумовлена багаторівневою системою механізмів та форм поведінки, сукупність яких має забезпечити інформаційну безпеку особистості, суспільства, держави.

Для вирішення проблем забезпечення інформаційної безпеки необхідною є комплексна система, що включає заходи виховного, освітнього характеру, їх популяризацію в масовій свідомості за допомогою всіх можливих засобів масової інформації та із застосуванням усіх найсучасніших інформаційних технологій, за активної участі держави. У цьому зв'язку слід описати основні рівні соціальних заходів інформаційної безпеки та напрями функціонування захисту, що дають уявлення про їх системний характер. Так, необхідно виділити три рівні організації соціальних заходів забезпечення інформаційної безпеки:

— у масштабах усього суспільства (макрорівень);

— у межах організацій та соціальних груп (мезорівень);

— на індивідуальному рівні (мікрорівень) [2; 4].

Перелічені рівні соціальних заходів інформаційної безпеки задають, відповідно, і основні напрями розвитку та функціонування забезпечення захисту.

На рівні суспільства в цілому або макрорівні соціальні заходи інформаційної безпеки реалізуються завдяки організації та регулюванню інформаційних потоків, а також поширенню засобів, способів та своєрідних "алгоритмів" оцінки, обробки інформації та застосування інформаційних технологій у процесі соціальної взаємодії від масової комунікації до міжособистісного спілкування. На цьому рівні суб'єктами захисту інформаційної безпеки виступають суспільство та держава у вигляді діяльності конкретних соціальних інститутів, що включають систему поширення соціальних норм, традицій, соціокультурних цінностей, систему освіти, формування сприятливої соціальної атмосфери, систему морального, правового регулювання тощо [3; 5].

На мезорівні соціальні заходи захисту реалізуються завдяки використанню та поширенню інформаційних джерел та специфічних способів соціальної взаємодії, оцінки та переробки інформації, характерних для конкретних організацій та соціальних груп. Тут можна виділити прийняті у різних соціальних групах чи професійних організаціях етичні норми, правила, регламентації, процедури інформаційної взаємодії та безпечного використання інформаційних технологій. До цього рівня належать такі суб'єкти захисту, як соціальні групи, виробничі структури, політичні, суспільні, релігійні та інші організації та об'єднання.

На мікро- чи індивідуальному рівні соціальні заходи забезпечення інформаційної безпеки здійснюються у процесі навчання та розвитку індивіда у вигляді створення специфічної регулятивної системи чи комплексу механізмів і алгоритмів, котрі визначають поведінку суб'єкта у інформаційному середовищі.

Визначивши структуру та зміст системи соціальних заходів забезпечення інформаційної безпеки, необхідно розглянути докладніше передбачені нею технології захисту [2; 4].

Так, у рамках державної політики на макрорівні соціальних заходів забезпечення інформаційної безпеки необхідно вжити наступних кроків:

— розробити узгоджену концепцію правового забезпечення інформаційної безпеки;

— запровадити практику популяризації основних принципів інформаційної безпеки, прав та обов'язків в інформаційній сфері;

— створити науково-методологічну базу у галузі інформаційної безпеки [2; 5].

Засоби масової інформації стають одними з ключових компонентів базисного ступеня інформаційної етики. У міру того, як зростає вплив інформаційної технології, система поширення інформації та соціокультурних цінностей повинна інформувати про проблеми інформаційної безпеки, права та обов'язки громадянина в даній сфері. Широкі верстви громадськості мають явно відчути те що, що інформаційна технологія може як завдавати шкоди цінностям людини, і просувати їх.

Максимальний ефект від зусиль, що докладаються на даному ступені популяризації знань з галузі інформаційної безпеки та інформаційної етики, може виражатися у збільшенні кількості соціальних суб'єктів, які, не будучи професіоналами у сфері інформаційних технологій, філософії, юриспруденції чи соціології, але набудуть здатності здійснювати попередні оцінки поведінки суб'єктів щодо ідентифікації соціальних та етичних проблем, що виникають.

Наступний ступінь — "теоретична" інформаційна етика, яка на заданому рівні покликана застосовувати наукові теорії до аналізу соціальних та етичних проблем, що виникають у суспільстві у процесі застосування інформаційних технологій [3—5].

Насправді жодна з цих щаблів популяризації етичного знання не має чітких кордонів, але всі перелічені "рівні аналізу" необхідні для досягнення головної мети — просування та захисту людських цінностей. Суспільство в особі кожного соціального суб'єкта має бути сприйнятливіше до всіх можливих наслідків використання інформаційної технології. Фахівці, які працюють у сфері інформаційних технологій, громадські діячі та політики, для підвищення ефективності результатів своєї діяльності повинні мати навички та знання, як мінімум передбачувані на другому ступені. У свою чергу, представники наукового середовища повинні продовжувати поглиблювати розуміння соціального та етичного впливу обчислювальної техніки, займаючись теоретичними аналізами та дослідженнями.

Крім того, важливим аспектом третьої умови (розробка науково-методологічної бази в галузі інформаційної безпеки) є створення педагогічних технологій щодо вивчення проблем інформаційної безпеки та формування інформаційної культури у процесі навчання у системі освіти. Забезпечення розробки та розповсюдження наукових, науково-популярних, навчально-методичних матеріалів та літератури з проблем інформаційної безпеки, інформаційної етики та інформаційної культури суспільства. Здійснення підготовки та підвищення кваліфікації педагогічних кадрів з метою організації навчального процесу на високому професійному рівні у системі освіти, які сприяють формуванню ефективної системи інформаційної безпеки [2; 4; 5].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Таким чином, державна політика забезпечення інформаційної безпеки зобов'язана включити в якості одного з пріоритетних напрямів своєї діяльності організацію та підтримку наукових досліджень у галузі розробки та впровадження інформаційних технологій, а також аналізу та прогнозу результатів її використання. Головною метою даних досліджень, заснованих на принципах інформаційної етики, насамперед мають стати узагальнення досвіду, формування моделей та теоретичних концепцій, формулювання рекомендацій для реалізації оптимальної системи інформаційної безпеки, прогнозування та нейтралізація можливих негативних ефектів застосування інформаційних технологій.

Література:

1. Семенець-Орлова І., Клочко А., Амро Т. Публічне управління у сфері інформаційної безпеки для забезпечення розвитку демократії в Україні (контекст воєнного стану). Публічне урядування. 2024. № 5 (33). С. 73—82.

2. Сердюк І. А. Підходи публічного управління до інформаційної безпеки особистості. Публічне урядування. 2022. № 3 (31). С. 53—59.

3. Ситник Г. П., Клименко Н. Г., Горєліков І. О. Державна політика забезпечення інформаційної безпеки та кібербезпеки, як її складової: проблеми та шляхи їх вирішення. Державне управління: удосконалення та розвиток. 2024. № 5. URL: http://nbuv.gov.ua/UJRN/Duur_2024_5_6.

4. Сілаєв В., Горінов П. Політика інформаційної безпеки в умовах цифрової трансформації України: виклики та шляхи попередження. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2024. № 3 (75). С. 81—87.

5. Торічний В. О. Формування та впровадження державної інформаційної політики як запорука забезпечення державної безпеки. Вісник Національного університету цивільного захисту України. Серія "Державне управління". 2019. Вип. 1 (10). С. 64—69.

References:

1. Savosko, T. (2024), "Features of the formation of state information policy", Aspekty publichnoho upravlinnia, vol. 12(1), pp. 22—28.

2. Semenets-Orlova, I., Klochko, A. and Amro, T. (2024), "Public administration in the field of information security to ensure the development of democracy in Ukraine (the context of martial law)", Publichne uriaduvannia, vol. 5 (33), pp. 73—82.

3. Serdiuk, I. A. (2022), "Public administration approaches to information security of the individual", Publichne uriaduvannia, vol. 3 (31), pp. 53—59, available at: http://nbuv.gov.ua/UJRN/Duur_2024_5_6 (Accessed 10 Jan 2026).

4. Silaiev, V. and Horinov, P. (2024), "Information security policy in the context of digital transformation of Ukraine: challenges and ways of prevention", Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia, vol. 3 (75), pp. 81—87.

5. Sytnyk, H. P., Klymenko, N. H. and Horielikov, I. O. (2024), "State policy of ensuring of information security and cybersecurity as its component: problems and ways to solve", Derzhavne upravlinnia: udoskonalennia ta rozvytok, vol. 5, available at: http://nbuv.gov.ua/UJRN/Duur_2024_5_6 (Accessed 10 Jan 2026).

Стаття надійшла до редакції 14.01.2026 р.