КОМПЛЕКСНИЙ ПІДХІД ЩОДО РОЗУМІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

COMPREHENSIVE APPROACH TO UNDERSTANDING INFORMATION SECURITY IN THE CONTEXT OF NATIONAL SECURITY

УДК 65.012.8:007+32(477)
DOI https://doi.org/10.32782/pma2663-5240-2023.38.30

Котляров В.О.
докторант
Національний авіаційний університет

Державна інформаційна політика являється важливою складовою зовнішньої і внутрішньої політики країни та охоплює всі сфери життєдіяльності суспільства. Бурхливий розвиток інформаційної сфери супроводжується появою принципово нових загроз інтересам особистості, суспільства, держави та її національній безпеці. У статті автором розглянуто складові державної інформаційної політики щодо забезпечення інформаційної безпеки країни і визначені основні напрями діяльності органів державної влади у цій сфері. Проаналізовані внутрішні та зовнішні інформаційні загрози національній безпеці України та шляхи гарантування інформаційної безпеки країни. Інформаційна безпека автором розглядається як складова національної безпеки країни, а також як глобальна проблема захисту інформації, інформаційного простору, інформаційного суверенітету країни та інформаційного забезпечення прийняття урядових рішень. Запропоновані підходи щодо забезпечення процесу безперервності функціонування системи інформаційної безпеки держави з метою моніторингу нових загроз, визначення ризиків та рівнів їх інтенсивності.

Визначено, що метою інформаційної боротьби є забезпечення переваги у вирішенні певних завдань однієї сторони над іншою за рахунок досягнення вищості на інформаційному рівні. Під інформаційним простором автором пропонується розуміти певне середовище, у якому здійснюється формування, збирання, збереження, опрацювання і поширення інформації. Доведено, що задоволення у будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави, а стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обґрунтованість рішень та дій, що приймаються.

Ключові слова: *держава, політика, безпека, загрози, ресурси, національна безпека, інформація, захист, мережа, глобалізація, технології.*

State information policy is an important component of the country's foreign and domestic policy and covers all spheres of society's life. The rapid development of the information sphere is accompanied by the appearance of fundamentally new threats to the interests of the individual, society, the state and its national security. The article examines the components of the state information policy on ensuring the information security of the country and identifies the main directions of activity of state authorities in this area. Analyzed internal and external information threats to the national security of Ukraine and ways to guarantee the country's information security. Information security is considered as a component of the country's national security, as well as a global problem of information protection, information space, information sovereignty of the country and information support for government decision–making. Proposed approaches to ensure the continuity of the state's information security system in order to monitor new threats, identify risks and levels of their intensity.

It was determined that the purpose of the information struggle is to ensure superiority in solving certain tasks of one side over the other due to the achievement of supremacy at the information level. The author proposes to understand the information space as a certain environment in which information is formed, collected, stored, processed and distributed. It has been proven that the satisfaction of information needs to any extent leads to the mastery of information about the surrounding world and the processes taking place in it, that is, awareness of the individual, society and the state, and the state of awareness determines the degree of adequacy of the subjects' perception of the surrounding reality and as a result – the validity of the decisions and actions taken.

Key words: *state, politics, security, threats, resources, national security, information, protection, network, globalization, technologies.*

Вступ. Глобалізація, що сприяє налагодженню зв'язків, поширенню відповідних цінностей на всі континенти, збільшенню транскордонних потоків, зближенню навіть самих віддалених куточків світу, змінює саму парадигму людського буття, формує глобальне інформаційне суспільство. Саме новизна, складність та унікальність процесу інформатизації суспільства, збільшення світового комп'ютерного парку, перехід на мережеві технології інформаційного обслуговування, запобігання формуванню терористичному середовища, медіа–тероризму, обумовлює необхідність нових підходів щодо розуміння національних інтересів як окремих країн так і інтересів світової спільноти в цілому.

Аналіз публікацій за тематикою дослідження. Різні аспекти проблем національної безпеки, включаючи проблеми комплексного підходу щодо розуміння інформаційної безпеки у контексті національної безпеки, розглядалися у наукових працях вітчизняних і зарубіжних дослідників: в Україні різним аспектам зазначених питань присвячені дослідження відомих вчених, серед них: О. Баранов, О. Гончаренко, В. Горбулін, А. Гуцал, Ю. Данько, В. Дереко, Є. Камінський, Б. Канцелярук, А. Литвиненко, Є. Макаренко, Я. Малик, В. Остроухов, Г. Перепелиця, С. Пирожков, Н. Резнік, Ф. Рудич, О. Соснін, О. Старіш та інші; у західній науці представляли предмет колишніх і сучасних досліджень роботи І. Валлерстайна,

Д. Гудбі, Д. Істона, Д. Кауфмана, Г. Моргентау, Дж. Ная, Т. Паркінсона, У. Оуенса та інших.

Виклад основного матеріалу. У найширшому плані національні інтереси держави включають широке коло інтелектуальних, історичних, моральних цінностей. Без врахування культурно–історичних традицій і національних цінностей розуміння міжнародної політики буде неповне. Г. Моргентау американський вчений справедливо вважає національну ідентичність невід'ємним елементом національного інтересу. У науковій літературі суспільний інтерес подається як усвідомлення потреби суб'єкта або соціальної спільноти, що випливає з умов їх існування та діяльності. У той же час інтерес – це відношення потреб до умов їх реалізації. Відповідно, національний інтерес є усвідомлення та відображення в діяльності його лідерів корінних потреб держави. Але національні інтереси потрібно захищати. І практика засвідчує, що у нинішніх умовах жодна з держав не в змозі захистити себе, свої інтереси, покладаючись лише на військово–технічні засоби. Це питання все більше потребує комплексного підходу, включаючи політичні, економічні, інформаційні механізми тощо. Тільки їх об'єднання в одне єдине ціле може дати очікуваний позитивний результат [1].

Тож існує два аспекти вивчення інформаційної безпеки в контексті національної безпеки. Це самостійний елемент національної безпеки будь–якої країни і водночас інтегрована складова будь–якої іншої безпеки: військової, економічної, політичної тощо. У цьому складність розгляду проблематики інформаційної безпеки. Часто предметом аналізу стає одна галузь, наприклад сфера масової інформації.

Під інформаційним простором пропонується розуміти певне середовище, у якому здійснюється формування, збирання, збереження, опрацювання і поширення інформації. Варто звернути увагу, що не вжито термін «використання інформації». Це зроблено свідомо, щоб вивести з інформаційного простору людину як суб'єкта, що споживає інформацію.

Інформаційна інфраструктура – це єдність наступних компонентів: системи виробництва інформаційних продуктів, системи доставки їх до споживача, системи виробництва засобів виробництва інформаційних продуктів та доставки їх, системи виробництва інформаційних технологій, системи накопичення і збереження інформаційного продукту або інформаційного ресурсу, тобто системи сервісного обслуговування елементів інфраструктури і, нарешті, системи підготовки кадрів [2].

Інформаційна безпека має три основні складові: конфіденційність, цілісність і доступність. Конфіденційність належить до захисту чутливої інформації від несанкціонованого доступу. Цілісність означає захист точності і повноти інформації і програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувача в потрібний для нього час.

Тож інформаційна безпека суспільства, держави характеризується ступенем їх захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи [3].

Розрізняють внутрішні та зовнішні джерела інформаційної безпеки. Під внутрішніми джерелами розуміють відсутність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації конституційних прав та свобод громадян, в тому числі в інформаційній сфері. вважають внутрішнім джерелом інформаційної небезпеки посилення організованої злочинності та збільшення кількості комп'ютерних злочинів, зниження рівня освіченості громадян, що суттєво ускладнює підготовку трудових ресурсів для використання новітніх технологій, в тому числі інформаційних. Недостатня координація діяльності вищого державного керівництва, органів влади та військових формувань в реалізації єдиної державної політики забезпечення національної безпеки теж можна вважати таким джерелом. До зовнішніх джерел належать діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь–якими структурами; культурна експансія у відношенні до конкретної країни.

Об'єктом методології інформаційної безпеки є інформаційні процеси в соціо- і соціотехнічних системах, предметом – дослідження механізмів інформаційного впливу на особистість, суспільство і державу, а також способів, методів, засобів та каналів реалізації загроз національним інтересам на інформаційному рівні. Основним завданням методології інформаційної безпеки є створення науково-методичних основ своєчасного виявлення потенційних інформаційних загроз у різних сферах діяльності та механізмів їх реалізації, а також попередження і нейтралізації [4].

Слід зазначити, що ядром методології інформаційної безпеки є поняття інформаційної боротьби, триєдина сутність якого відображена в наступних взаємопов'язаних визначеннях:

• інформаційна боротьба – це об'єктивно існуюча форма прояву відносин між суб'єктами при вирішенні ними завдань, що містять елементи конфліктності різної природи на інформаційному рівні;

• інформаційна боротьба – це наука про механізми, прийоми, методи і засоби інформаційного протиборства;

• інформаційна боротьба – це комплекс заходів, спрямованих на вирішення завдань, що стоять перед суб'єктом, методами і засобами боротьби [5].

Існування інформаційної боротьби обумовлене як існуванням інформації, так і природністю процесу її використання, її властивостей для вирішення різних завдань. Із визначення інформаційної боротьби випливає, що вона, на відміну від інформаційної війни, по суті своїй неагресивна. До її методів і засобів вдаються, наприклад, з метою обґрунтування доцільності впровадження у виробництво певних технологічних рішень. Як об'єктивно існуючий феномен інформаційна боротьба має свої цілі, завдання, законом інформаційні ресурсної, способи, методи і засоби її ведення.

Метою інформаційної боротьби є забезпечення переваги у вирішенні певних завдань однієї сторони над іншою за рахунок досягнення вищості на інформаційному рівні. Цієї мети можна досягти різними шляхами:

1. Цілеспрямоване добування інформації про поточну ситуацію з жорсткими вимогами щодо її своєчасності, якості, обсягу, повноти і темпів оновлення, оцінка на основі цієї інформації політичної (військово–політичної, військової, економічної, екологічної тощо) ситуації. Вирішення цього комплексу завдань ускладнюється тим, що воно здійснюється в умовах інформаційної протидії. При цьому інформація, що аналізується, відзначається непевністю об'єктивного і суб'єктивного характеру, неповнотою щодо одних аспектів до інших, суперечливістю, наявністю частково зруйнованої та спотвореної інформації, у тому числі і дезінформації.

2. Цілеспрямований і комплексний вплив на свідомість, інформаційні ресурси країни на всіх етапах їхнього виробництва, поширення і використання, а також на інформаційну сферу машинно–технічних систем протиборчої (конкуруючої) сторони з метою нав'язування «бажаних» рішень і «керування поведінкою». При цьому особливої важливості набуває не стільки руйнівна, скільки цілеспрямована впливова дія щодо спотворення змісту інформації для забезпечення своїх інтересів у різних сферах діяльності особистості, суспільства, держави. У цьому контексті особливої значущості набуває можливість використання інформації (інформаційних потоків) як ефективного засобу формування позитивного іміджу України на міжнародній арені та можливість зняття політичної, економічної, соціальної, військово–політичної, особливо ж військової напруженості у взаємовідносинах з іншими країнами, а також у різних регіонах держави.

3. Захист власних інформаційних ресурсів та інфосфери машинно–технічних систем од впливу на них протиборчої сторони. Анітрохи не применшуючи важливості вирішення завдань технічного захисту інформації, спрямованої в основному на забезпечення її конфіденційності, варто підкреслити особливу значимість захищеності змісту інформації від навмисного його спотворення або зміни, в тому числі і механізмів виявлення дезінформації. До цього ж комплексу входять також і завдання відновлення цілісності змісту частково зруйнованої або перекрученої текстової природно–мовної інформації [6].

Як вже зазначалося в об'єктами інформаційної безпеки можуть бути: свідомість, психіка людей; інформаційні системи різного масштабу і різного призначення. До соціальних об'єктів інформаційної безпеки звичайно відносять особистість, колектив, суспільство, державу, світове товариство [7].

До суб'єктів інформаційної безпеки відносяться:

• держава, що здійснює свої функції через відповідні органи;

• громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства.

Згадаємо, що інформаційна безпека особистості – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування тощо [8].

Інформаційна безпека держави (суспільства) характеризується ступенем захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси тощо) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

В узагальненому виді інформаційна безпека держави – представляє собою систематизовану сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення.

У концептуальному плані інформаційна безпека держави включає:

• системну класифікацію дестабілізуючих чинників і інформаційних загроз безпеці особистості, суспільства і держави;

• обґрунтування основних положень з організації забезпечення інформаційної безпеки держави;

• розробку пропозицій та рекомендацій, що включають засоби і форми забезпечення інформаційної безпеки.

Поняття інформаційної безпеки, залежно від його використання, розглядається у декількох ракурсах.

У найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [9].

Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні предметні частини:

• створення і розповсюдження вихідної та похідної інформації;

• формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;

• споживання інформації;

• та дві забезпечувальні предметні частини:

• створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;

• створення і застосування засобів і механізмів інформаційної безпеки.

Більш розгорнуте формулювання інформаційної безпеки – це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [10].

Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обґрунтованість рішень та дій, що приймаються.

У залежності від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати наступним чином:

• як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;

• інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;

• інформаційних прав і свобод людини і громадянина.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [11].

Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері. Відповідно до загально визнаних підходів, інтереси особистості в інформаційній сфері полягають:

• у реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку;

• у захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають:

• у забезпеченні інтересів особистості в цій сфері;

• у зміцненні демократії;

• у створення правової соціальної держави;

• у досягненні та підтриманні суспільного спокою;

• у духовному відновленні держави.

Інтереси держави в інформаційній сфері полягають у створенні умов:

• для гармонійного розвитку державної інформаційної інфраструктури;

• для реалізації конституційних прав і свобод людини та громадянина в галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Висновки та перспективи подальших розвідок. Таким чином, серед зарубіжних та вітчизняних науковців існує декілька підходів

до визначення поняття інформаційна безпека: факторний, ціннісний, та методологічний. Зокрема, у межах методологічного підходу поняття «національна безпека» розподіляється на три групи: нормативно–правова, доктринальна та енциклопедична [12].

Факторний підхід включає до себе сукупність чинників, що впливають на інформаційну безпеку: а) глобалізація інформаційного простору, телекомунікаційних мереж та інформаційних ринків; б) перехід суспільства в фазу інформаційного розвитку; в) формування громадянського суспільства. І нарешті, ціннісний підхід полягає в тому, що проблему інформаційного впливу на індивідуальну, масову і суспільну свідомість, культуру і психіку людей варто розглядати не у площині забезпечення інформаційної безпеки, а як питання психічної та духовної безпеки [13].

Отже, історична практика увібрала до себе багато підходів щодо розуміння інформаційної безпеки як окремої людини, суспільства, держави. Проте епоха глобального розвитку комп'ютерних технологій, засобів електронної комунікації, інформаційних війн, геополітичної конкуренції заставляють шукати нові підходи, нові важелі та інструментарій для безпечного розвитку людської спільноти.

ЛІТЕРАТУРА:

1. Домарєв В.В., Домарєв Д.В., Гордієнко С.Б. Обґрунтування основних функцій системи управління інформаційною безпекою. *Вісник Державного університету інформаційно-комунікаційних технологій.* № 10(2). 2012. С. 102–104.

2. Домарев В. В. Безпека інформаційних технологій. *Методологія створення систем захисту.* 2013. 688 с.

3. Заник О., Ткачук Р. Вплив людського фактору на системи організації інформаційної безпеки. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів *«Інформаційна безпека та інформаційні технології»*. 26. 11. 2020 р. Львів : ЛДУБЖД, 2020. С. 21–22.

4. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання. *Економіка в контексті глобальних змін суспільства* : матеріали Міжнародної науково-практичної конференції. 18 липня 2020 р. Дніпро : НО «Перспектива». 2020. С. 100–104.

5. Інформаційна безпека (соціально-правові аспекти) [В. Остроухов, В. Петрик, М. Присяжнюк та ін.]; за ред. Є.Д. Скулиша. К. : КНТ, 2010. 776 с.

6. Євсєєв С. Оцінка забезпечення безперервності бізнес-процесів в організаціях банківського сектора на основі синергетичного підходу. *Сучасна спеціальна техніка.* Науково-практичний журнал. 2017. № 2. С. 10–17.

7. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2015. № 2 (18). С. 16–22.

8. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України. Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів *«Проблеми та перспективи розвитку системи безпеки життєдіяльності»*. 23–24 березня 2017 р. [в 2 ч.]. Ч. 2. Львів: ЛДУ БЖД, 2017. С. 11–12.

9. Хох В.Д., Мелешко Є.В., Смірнов О.А. Дослідження методів аудиту систем управління інформаційною безпекою. *Системи управління, навігації та зв'язку.* №1(41) 2017. С. 39–42.

10. Малик Я. Інформаційна війна і Україна. Демократичне врядування. 2015. Вип. 15. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3 (дата звернення: 10.10.2022).

11. Цуркан В.В. Метод функціонального аналізування систем управління інформаційною безпекою. Кібербезпека: освіта, наука, техніка. № 4(8). 2020. С. 192–201.

12. Цвид–Гром О.П., Скляренко Т.І. Упровадження ECM–системи як інтегрованої платформи під час роботи з корпоративним контентом. *Соціальні комунікації: теорія і практика.* 2016. С. 104.

13. Остроухов В.В. Інформаційна безпека. URL: http://westudents.com.ua/glavy/51894-12-nformatsyna-vyna-yak-forma-vedennya-nformatsynogoprotiborstva.html (дата звернення: 12.04.2022).

14. Danko Y. I. & Reznik N. P. (2019). Contemporary challenges for China and Ukraine and perspectives for overcoming these challenges. *Global Trade and Customs Journal*, 14(6).

15. Reznik N., Hridin O., Chukina I., Krasnorutskyy O., Mykhaylichenko M. (2022). Mechanisms and tools of personnel management in institutional economics. AIP Conference Proceedings. 2413, 040012 https://doi.org/10.1063/5.0089330.