УДК 351.746.1:004.056(045)

О. І. Кравченко,
аспірант кафедри публічного управління та адміністрування,
Національний авіаційний університет.
ORCID ID: https://orcid.org/0009-0006-0759-6830

DOI: 10.32702/2306-6814.2023.18.229

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

A. Kravchenko,
Postgraduate student of the Department of Public Administration,
National Aviation University

INFORMATION SECURITY AS A COMPONENT OF NATIONAL SECURITY

У статті розглянуто наукові підходи до визначення поняття "інформаційна безпека" як складової національної безпеки. Визначено основні завдання інформаційної безпеки, виконання яких дасть можливість забезпечити інформаційний простір країни від неправдивої, неточної інформації та зберегти інформаційний суверенітет країни. Виявлено особливості інформаційних загроз, які існують у різних сферах діяльності (політичній, економічній, суспільній, військовій та науково-технічній) та впливають на стан національної безпеки.

Розглянуто нормативно-правові документи, прийняті для забезпечення інформаційної безпеки та реалізації інформаційної політики держави в умовах воєнного часу. Проаналізовано методи протидії інформаційним загрозам (превентивні та оперативні), використання яких дасть можливість не допускати виникнення інформаційної загрози та попередити її формування на початковому етапі. Запропоновано варіанти забезпечення інформаційної безпеки, зокрема необхідність створення власної моделі інформаційного простору державного рівня та забезпечення розвитку інформаційного суспільства; підвищення конкурентоспроможності власної інформаційної продукції та інформаційних послуг, а також інтегрування України до міжнародного інформаційного простору.

The article examines the categorical and conceptual apparatus related to ensuring information security as a component of national security. Scientific approaches to defining the concept of "information security" are revealed. It has been established that information security is considered as a state of protection of the information space and the national interests of the country in this space; the process of managing information threats and dangers to ensure the information sovereignty of the state; functions of the state; a component of national security.

The main tasks of information security have been determined, the implementation of which will make it possible to ensure the country's information space from false and inaccurate information and preserve the country's information sovereignty.

The specifics of information threats that exist in various spheres of activity (political, economic, social, military, and scientific and technical), which generally affect the state of national security, have been identified. In particular, the position is given that the main information threat in the field of national security is the threat of negative external influence on the information environment of the country, the information consciousness and subconsciousness of a person with the aim of imposing one's own views, values and positions to control the behavior of society. It has been proven that in fact such external negative influence is a real threat to the country's sovereignty, especially in wartime conditions.

The methods of countering information threats (preventive and operative) have been analyzed, the use of which will make it possible to prevent the emergence of an information threat and to prevent its formation at the initial stage, using means and resources for its neutralization.

The regulatory documents adopted to ensure information security and the implementation of information policy in wartime conditions are considered. It has been established that the change in the legislation provides for the prohibition of dissemination during martial law of information of a dangerous nature for society, and the establishment or strengthening of various types of liability for violation of such a prohibition.

Attention is focused on the need to ensure information security in the conditions of a hybrid war, in particular by creating an own model of the information space at the state level and ensuring the development of an information society; increasing the competitiveness of its own information products and information services, as well as the integration of Ukraine into the international information space.

Ключові слова: державна політика, інформація, інформаційна безпека, національна безпека, інформаційний суверенітет, інформаційні загрози, інформаційний простір.

Key words: public policy, information, information security, national security, information sovereignty, information threats, information space.

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

Сьогодні перед нашою країною стоїть надзвичайно важливе завдання із забезпечення національної безпеки та державного суверенітету, адже саме від цього залежить розвиток суспільства та функціонування держави. В умовах російської військової агресії нового змісту та особливостей набуває інформаційна війна, результати якої зокрема впливають на маніпулювання свідомістю громадян та розпалювання між ними недовіри та ворожнечі; дезінформація про роботу органів влади та їх дискредитація; ініціювання масових заворушень, мітингів та страйків тощо.

Тому в умовах російсько-української війни досить актуальним залишається питання розгляду інформаційної безпеки як складової національної безпеки України.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Зазначена проблематика перебуває в полі зору багатьох учених. Зокрема різні аспекти та особливості забезпечення інформаційної безпеки висвітлювали у своїх наукових працях такі автори як: І. Боднар, С. Глобенко, У. Ільницька, В. Кононенко, В. Кривцов, Н. Литвин, Т. Слінько, Т. Ткачук, Я. Чмир, О. Штельмах та інші.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою даної статті є дослідження особливостей інформаційної безпеки як складової національної безпеки країни.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Сьогодні для більшості країн світу питання забезпечення національної безпеки є пріоритетним, адже від цього залежить економічний розвиток країни та добробут її населення. Сама ж система національної безпеки поєднує в собі різні сфери безпеки, зокрема політичну, військову, кадрову, економічну, екологічну, соціальну, продовольчу і, звичайно ж, інформаційну [12].

Відповідно в умовах російської військової агресії Україна більш активно здійснює різноманітні заходи для забезпечення своєї національної безпеки. Одними з таких заходів є забезпечення інформаційної безпеки шляхом формування ефективної державної інформаційної політики на засадах демократичної правової держави із розробкою та прийняттям нормативно-правових документів, зокрема національних доктрин, стратегій, концепцій та програм.

У сучасних реаліях ми бачимо, що роль інформації, спосіб її висвітлення та представлення громадськості є надзвичайно важливою, оскільки вона фактично є інформаційною зброєю. Інформація може формувати та розпалювати у суспільстві як внутрішні протиріччя, так і протиріччя та війни між країнами, або ж дозволяє встановлювати дружні стосунки [17].

На основі аналізу літературних джерел встановлено, що одні науковці вважають інформаційну безпеку — станом захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [10]. Інші вчені трактують інформаційну безпеку як стан інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації і захист суб'єктів від негативної інформаційної дії [11].

У той же час, на думку Кривцова В. Ю., інформаційну безпеку можна розглядати як стан захищеності інформаційного простору та національних інтересів країни в цьому просторі; процес управління інформаційними загрозами та небезпеками для забезпечення інформаційного суверенітету держави; функції держави; складової частини національної безпеки [8].

Слід акцентувати увагу на тому, що Конституцією України передбачено, що найважливішими функціями дер-

жави є захист її суверенітету і територіальної цілісності, а також забезпечення інформаційної безпеки держави.

У той же час, у Стратегії інформаційної безпеки наведено наступне трактування поняття "інформаційна безпека України" — це "складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії завданню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом" [13].

Ми дотримуємося думки про те, що інформаційна безпека — це збалансований стан функціонування та взаємодії інститутів громадянського суспільства та держави, з метою формування та розвитку інформаційного середовища в інтересах людини, суспільства та держави, а також досягнення мінімізації впливу в інформаційному просторі негативних чинників на національні інтереси держави та її громадян. Отже забезпечення інформаційної безпеки включає не тільки забезпечення інтересів країни, а й інтересів, прав і свобод кожного її громадянина. Ми підтримуємо думку науковців, що достовірність, точність, доступність інформації, контроль за її правдивістю та непоширеністю дезінформації, захист інформаційного простору від маніпуляцій є основою інформаційної безпеки сьогодення [17].

Аналіз літературних джерел та нормативно-правових документів дає нам можливість стверджувати, що основними завданнями інформаційної безпеки є [8, 13, 15]:

— створення умов для забезпечення інформаційного суверенітету України шляхом формування та реалізації державної політики інформаційної безпеки, а також формування нормативно-правової бази та економічних чинників для розвитку інформаційного середовища та інформаційної інфраструктури;

— здійснення ефективних заходів щодо наповнення інформаційного простору достовірною інформацією про Україну, у т.ч. шляхом залучення засобів масової інформації та недопущення втручання у їх діяльність, переслідування чи дискримінації, а також забезпечення захисту інформаційного простору від монополізації;

— проведення постійного моніторингу стану інформаційної безпеки для попередження шкідливого впливу загроз і небезпек як всередині країни, так і ззовні, у т.ч. виявлення та запобігання інформаційної небезпеки та інформаційних атак на діяльність органів публічної влади тощо.

Виділяють чотири групи інформаційних небезпек для суспільства і держави, які виникають у наслідок розвитку науково-технічного прогресу [3]:

1) розвиток програмування (комп'ютерна система банків даних знань і інформаційні ресурси, комп'ютерні ігри) здатний впливати на людську психіку і інформаційно-технологічні державні структури;

2) формування нового виду правопорушень: махінації з банківськими операціями; порушення порядку у комп'ютерній сфері; протизаконне копіювання технологічних рішень тощо;

3) постійний електронний контроль стану життя населення країни (здоров'я, активність соціального плану, політичні настрої, відносини між людьми, фінансове забезпечення громадян) через використання інформаційних технологій;

4) підвищення впливу ЗМІ на політичні процеси, роботу владного механізму.

Отже, як бачимо, в умовах науково-технічного прогресу, використання комп'ютерної техніки, соціальних мереж потенційна вразливість суспільства та суспільних процесів від інформаційного впливу надзвичайно зростає. Інформація та спосіб її подачі може призвести до великомасштабних аварій, військових конфліктів, дезорганізації публічного управління тощо.

Інформаційна небезпека виникає у разі появи інформаційних загроз. З науково-технічним суспільства кількість таких загроз постійно зростає. Слід звернути увагу на те, що інформаційним загрозам у сфері національної безпеки приділено значну уваги як науковців, так і практиків. Зокрема у Доктрині інформаційної безпеки України передбачено такі загрози як [15]:

— здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності країни та створення її негативного іміджу;

— дестабілізація у суспільстві через політичні та міжетнічні конфлікти в Україні;

— інформаційне домінування та інформаційна експансія державою-агресором;

— недостатній рівень протидії інформаційній агресії;

— неефективність наявної державної інформаційної політики, зокрема недосконалість чинного законодавства, невизначеність або взагалі відсутність стратегічного наративу, недостатній рівень медіа-культури суспільства тощо.

У той же час науковці виокремлюють наступні загрози національній безпеці в інформаційній сфері [2, 7]:

— недосконалість нормативно-правового забезпечення щодо регулювання та унормовування питань у сфері інформаційної безпеки, особливо на місцевому рівні;

— недостатній рівень розвитку на місцевому та державному рівні інформаційно-телекомунікаційної інфраструктури, зосередження засобів масової інформації в руках певних зацікавлених осіб;

— непослідовність та неефективність державної політики щодо здійснення якісних заходів із забезпечення інформаційної безпеки;

— ведення інформаційної війни проти України, особливо в умовах повномасштабного вторгнення росії;

— дезінформація громадян України та застосування проти них технологій інформаційно-психологічного маніпулятивного характеру.

Заслуговує на увагу і той факт, що інформаційні загрози із зовнішніх джерел є найбільш небезпечними у сфері національної безпеки нашої країни. Зокрема до таких загроз ми можемо віднести: недостатність поінформованості населення, яке перебуває за межами України,

про ведення зовнішньополітичної та внутрішньополітичної діяльності країни; дезінформування щодо ведення зовнішньої та внутрішньої політики України; інформаційний вплив міжнародних структур та організацій у різних сферах (військовій, економічній, політичній, інформаційній) на формування структури політичної системи в Україні, розроблення і реалізацію політичних рішень; утиски інформаційних прав та свобод, що зазнають українські громадяни поза межами країни.

Деякі науковці вважають, що загрози інформаційній безпеці призводять до порушення нормальної життєдіяльності окремої людини та країни в цілому, а також до руйнації або стримування розвитку інформаційної інфраструктури. [1].

Ми дотримуємося тієї точки зору, що головною інформаційною загрозою у сфері національної безпеки є загроза негативного стороннього впливу на інформаційне середовище країни, інформаційну свідомість та підсвідомість людини з метою нав'язування власних поглядів, цінностей та позицій для керування поведінкою суспільства. Фактично такий сторонній негативний вплив є реальною загрозою для суверенітету країни, особливо в умовах війни.

Не можна залишити поза увагою і те, що інформаційні загрози існують у різних сферах діяльності, зокрема у політичній; економічній; суспільній; військовій та науково-технічній [18].

Так, у політичній сфері інформаційні загрози впливають на функціонування системи державного управління; на систему підготовки прийняття та впровадження політичних рішень; на виборчі системи та процедуру проведення виборів тощо.

В економічній сфері інформаційні загрози накладають відбиток на ефективність функціонування банківської системи та управління корпоративними правами (можливе виникнення корпоративних війн, банківського шпіонажу і хакерських атак).

У суспільній сфері інформаційні загрози впливають на систему формування громадської думки; структури формування політичних партій, громадських рухів та релігійних організацій; структури забезпечення основних прав і свобод людини. Це призводить до загроз конституційним правам і свободам людини.

У військовій сфері інформаційні загрози призводять до фальсифікації фактів військової історії; напруженості та дестабілізації ситуації в місцях дислокації військових; військових злочинів та дезертирства, а також втрати бойового духу та підриву обороноздатності країни.

У науково-технічній сфері інформаційні загрози можуть впливати на системи накопичення ноу-хау та об'єкти інтелектуальної власності; структури фундаментальних і прикладних досліджень; бази і банки даних конфіденційного характеру.

Для протидії інформаційним загрозам слід використовувати превентивні методи (нормативно-правові, адміністративні, інформаційні та економічні), що дасть можливість не допустити інформаційної загрози та попередити ризики на початкових етапах, а також оперативні методи, які можна застосувати тільки після виявлення правдивих та перевірених даних щодо наявності інформаційної загрози, її рівня та можливих засобів і ресурсів для її нейтралізації [18].

Варто акцентувати увагу на тому, що для забезпечення інформаційної безпеки в Україні та протидії застосуванням технологій гібридної війни з боку росії, які впливають на свідомість людини, розпалювання релігійної ворожнечі, зміну конституційного ладу незаконним та насильницьким методам, а також порушення суверенітету, незалежності та територіальної цілісності України було прийнято Доктрину інформаційної безпеки України [15]. З моменту впровадження воєнного стану в Україні, прийнято рішення Ради національної безпеки та оборони України "Щодо реалізації єдиної інформаційної політики в умовах воєнного стану", в основі якого пріоритетним питанням національної безпеки є реалізація єдиної інформаційної політики та створення і функціонування Центру протидії дезінформації при РНБО України [14]. Враховуючи те, що країна-агресор здійснює свій інформаційний вплив на населення, надаючи неправдиву інформацію, безпосередньо через телекомунікаційні засоби в Україні, було прийнято рішення про об'єднання всіх загальнонаціональних телеканалів, які на базі єдиної інформаційної стратегічної комунікації здійснюють транслювання своїх інформаційно-аналітичних передач [9]. Відбувається постійний моніторинг та контроль ефірних мереж для виявлення ворожої неправдивої інформації та несанкціонованого втручання. Ми погоджуємося, що саме фільтрування інформації в такий спосіб є одним із заходів державного контролю та запобігання фізичній і моральній загрозам.

Також прийнято певні нормативно-правові документи, які передбачають заборону розповсюдження під час воєнного стану інформації, що має небезпечний характер для суспільства та встановлення або посилення різного виду відповідальності за порушення такої заборони. Наприклад, на законодавчому рівні посилено кримінальну відповідальність за виготовлення та розповсюдження під час воєнного стану забороненої продукції [17].

Однак, незважаючи на значну кількість прийнятих нормативно-правових документів, які регулюють питання інформаційної безпеки, все ж таки залишаються досить великі прогалини у законодавстві. Зокрема не відображена у нормативних документах класифікація явищ інформаційного простору, що призводить до ускладнення притягнення до відповідальності за вчинення будь-яких дій чи організацію діяльності, яка може завдати шкоди інформаційній безпеці.

Для попередження існуючих загроз та наявних проблем, крім удосконалення існуючої нормативно-правової бази відповідно до міжнародного законодавства, варто здійснювати заходи щодо створення власної моделі інформаційного простору державного рівня та забезпечення розвитку інформаційного суспільства; підвищення конкурентоспроможності власної інформаційної продукції та інформаційних послуг, а також інтегрування України до міжнародного інформаційного простору.

Потрібно постійно здійснювати контроль інформаційного простору, у т.ч. за діяльністю ЗМІ (преса, телебачення, радіо, Інтернет), інформацією, яку вони подають та способом її подачі. Крім того, необхідно здійснити заходи щодо обмеження розповсюдження інформації, яка шкодить авторитету діяльності уряду та Збройним Силам України серед населення країни або сприяє діяльності суперника (ворога).

Тому забезпечення інформаційної безпеки як складової національної безпеки в умовах військової агресії повинно відбуватися шляхом формування дієвої та ефективної державної політики, яка буде спрямована на захист людини, суспільства та держави в інформаційному середовищі. При цьому у процеси розробки та реалізації такої політики мають бути впровадженні та використовуватися сучасні інформаційні та комунікативні технології. Така державна політика в аспекті забезпечення інформаційної безпеки буде ефективна при взаємодії та тісній співпраці між органами публічної влади та інститутом громадянського суспільства.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Встановлено, що інформаційна безпека розглядається як стан захищеності інформаційного простору та національних інтересів країни у ньому; як процес управління інформаційними загрозами та небезпеками для забезпечення інформаційного суверенітету держави та її національної безпеки.

Визначено основні завдання інформаційної безпеки, реалізація яких дасть змогу убезпечити інформаційний простір країни від неправдивої та недостовірної інформації, зберегти інформаційний суверенітет країни.

Розкрито специфіку інформаційних загроз, що існують у різних сферах діяльності (політичній, економічній, соціальній, військовій та науково-технічній) та які в цілому впливають на стан національної безпеки. Зокрема, наводиться положення про те, що основною інформаційною загрозою у сфері національної безпеки є загроза негативного зовнішнього впливу на інформаційне середовище країни, інформаційну свідомість та підсвідомість особи з метою нав'язування власних поглядів, цінностей та позиції для контролю поведінки суспільства. Доведено, що насправді такий зовнішній негативний вплив є реальною загрозою суверенітету країни, особливо в умовах воєнного часу.

Проаналізовано методи протидії інформаційним загрозам (превентивні та оперативні), використання яких дасть змогу запобігти виникненню інформаційної загрози та запобігти її формуванню на початковому етапі, використовуючи засоби і ресурси для її нейтралізації.

Розглянуто прийняті нормативні документи щодо забезпечення інформаційної безпеки та реалізації інформаційної політики в умовах воєнного часу. Встановлено, що зміна до законодавства передбачає заборону поширення під час дії воєнного стану інформації суспільно небезпечного характеру та встановлення чи посилення різних видів відповідальності за порушення такої заборони.

Запропоновано для забезпечення інформаційної безпеки як складової національної безпеки забезпечувати формування дієвої та ефективної державної політики, здійснювати постійний контроль інформаційного простору, а також має бути тісна співпраця та взаємодія між органами публічної влади та інститутом громадянського суспільства. Досить важливо здійснювати заходи щодо створення власної моделі інформаційного простору державного рівня та забезпечення розвитку інформаційного суспільства; підвищення конкурентоспроможності власної інформаційної продукції, інформаційних послуг, а також інтегрування України до міжнародного інформаційного простору.

Література:

1. Боднар І. Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68—75.

2. Глобенко С. Інформаційний простір держави та проблеми забезпечення його захисту в Україні. Державне управління. 2023. № 1 (13). С. 195—210.

3. Гриненко І. М., Прокоф'єва-Янчиленко Д. М., Сокрут Б. В. Ризики та загрози організованої злочинності в Україні: стан та перспективи / І. М. Гриненко, Д. М. Прокоф'єва-Янчиленко, Б. В. Сокрут, Київ: ВАІЕУ, 2014. 194 с.

4. Грицай Р. О. Інформаційні війни: пошук стратегій протидії. Публічне управління і адміністрування в Україні. 2023. Вип. 33. С. 18—23.

5. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним викликам. Політичні науки. 2016. № 1. Вип. 2. С. 27—32.

6. Кононенко В. П., Здоровко С. С., Корольова А. Є. Інформаційна безпека як стан. Науковий вісник Ужгородського національного університету. 2023. Вип. 7. Ч. 2. С. 244—250.

7. Копанчук В. О. Державна політика у сфері національної безпеки та охорони громадського порядку: дис.... докт. держ. упр.: спец. 25.00.05. "Держ. упр. у сфері держ. безпеки та охорони гром. порядку" / НУЦЗУ. Харків, 2020. 375 с.

8. Кривцов В. Ю. Інформаційні заходи оборони держави в сучасних умовах. Часопис Київського університету права. 2023. № 1. С. 30—33.

9. Литвин Н А., Шевченко А. О. Діяльність органів державної влади щодо забезпечення інформаційної безпеки України під час війни: адміністративно-правовий аспект. Юридичний науковий електронний журнал. 2023. № 1. С. 299—302.

10. Лук'янова В. В., Лаутар А. Ю. Інформаційна безпека в умовах розвитку інформаційної системи. Вісник Хмельницького національного університету. 2013. № 2. Т. 3. С. 97—101.

11. Панченко А. О., Панченко Л. В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. Правова інформатика. 2015. № 2 (46). С. 32—38.

12. Пархоменко-Куцевіл О. Проблеми забезпечення національної безпеки в умовах воєнного часу. Науковий вісник Вінницької академії безперервної освіти. 2023. Вип. 3. С. 143—150.

13. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28 грудня 2021 року № 685. URL: https://www.president.gov.ua/documents/6852021-41069

14. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року "Щодо реалізації єдиної інформаційної політики в умовах воєнного стану": Указ Президента України від 19 березня 2022 року № 152. URL: https://zakon.rada.gov.ua/go/152/2022.

15. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України": Указ Президента України від 25 лютого 2017 року №47/2017. URL: https://www.president.gov.ua/documents/472017-21374

16. Слінько Т. Сучасні загрози інформаційній безпеці країни й шляхи їх подолання. Український часопис конституційного права. 2021. № 4. С. 77—84.

17. Смотрич Д. В., Браілко Л. Інформаційна безпека в умовах воєнного стану. Науковий вісник Ужгородського національного університету. 2023. С. 121—127.

18. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Підприємництво, господарство і право. 2017. № 10. С. 182—186.

19. Ткачук Т. Ю. Механізми протидії інформаційним загрозам зовнішніх джерел. ВІСНИК НТУУ "КПІ". Політологія. Соціологія. Право. 2017. Вип. 1/2. С. 242—254.

20. Чмир Я. Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення. Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління. 2022. Вип. 2 (62). С. 149—154.

21. Штельмах О. В. Організаційні аспекти протидії інформаційній агресії як складової гібридної війни. Актуальні проблеми управління державною безпекою: зб. матер. наук.-практ. конф (Київ, 19 березня 2015). К.: Центр навч., наук, та період, видань НА СБ України, 2015. С. 393—396.

References:

1. Bodnar, I. R. (2014), "Information security as the basis of national security", Mekhanizm rehuliuvannia ekonomiky, vol. 1, pp. 68—75.

2. Hlobenko, S. (2023), "Information space of the state and problems of ensuring its protection in Ukraine", Derzhavne upravlinnia, vol. 1 (13), pp. 195—210.

3. Hrynenko, I. M. Prokof'ieva-Yanchylenko, D. M. and Sokrut, B. V. (2014), Ryzyky ta zahrozy orhanizovanoi zlochynnosti v Ukraini: stan ta perspektyvy [Risks and threats of organized crime in Ukraine: state and prospects], VAIEU, Kyiv, Ukraine.

4. Hrytsaj, R. O. (2023), "Information wars: search for countermeasure strategies", Publichne upravlinnia i administruvannia v Ukraini, vol. 33, pp. 18—23.

5. Il'nyts'ka, U. (2016), "Information security of Ukraine: modern challenges, threats and countermeasures against negative information and psychological challenges", Politychni nauky, vol. 2, pp. 27—32.

6. Kononenko, V. P. Zdorovko, S. S. and Korol'ova, A. Ye. (2023), "Information security as a state", Naukovyj visnyk Uzhhorods'koho natsional'noho universytetu, vol. 7, pp. 244—250.

7. Kopanchuk, V. O. (2020), "State policy in the field of national security and protection of public order", Abstract of Ph.D. dissertation, State administration in the field of state security and protection of public order, National university of civil defense of Ukraine, Kharkiv, Ukraine.

8. Kryvtsov, V. Yu. (2023), "Information measures of state defense in modern conditions", Chasopys Kyivs'koho universytetu prava, vol. 1, pp. 30—33.

9. Lytvyn, N A. and Shevchenko, A. O. (2023), "Activities of state authorities to ensure information security of Ukraine during the war: administrative and legal aspect", Yurydychnyj naukovyj elektronnyj zhurnal, vol. 1, pp. 299—302.

10. Luk'ianova, V. V. and Lautar, A. Yu. (2013), "Information security in the conditions of information system development", Visnyk Khmel'nyts'koho natsional'noho universytetu, vol. 2, pp. 97—101.

11. Panchenko, A. O. and Panchenko, L. V. (2015), "Information security and information culture in the modern information society", Pravova informatyka, vol. 2 (46), pp. 32—38.

12. Parkhomenko-Kutsevil, O. (2023), "Problems of ensuring national security in wartime conditions", Naukovyj visnyk Vinnyts'koi akademii bezperervnoi osvity, vol. 3, pp. 143—150.

13. The President of Ukraine (2021), The decree "On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On Information Security Strategy", available at: https://www.president.gov.ua/ documents/6852021-41069 (Accessed 23 August 2023).

14. The President of Ukraine (2022), The decree "On the decision of the National Security and Defense Council of Ukraine dated March 18, 2022 "Regarding the implementation of a unified information policy under martial law", available at: https://zakon.rada.gov.ua/go/152/2022 (Accessed 23 August 2023).

15. The President of Ukraine (2017), The decree "On the decision of the National Security and Defense Council of Ukraine dated December 29, 2016 "On the Information Security Doctrine of Ukraine", available at: https://www.president.gov.ua/documents/472017-21374 (Accessed 23 August 2023).

16. Slin'ko, T. (2021), "Modern threats to the country's information security and ways to overcome them", Ukrains'kyj chasopys konstytutsijnoho prava, vol. 4, pp. 77—84.

17. Smotrych, D. V. and Brailko L. (2023), "Information security under martial law", Naukovyj visnyk Uzhhorods'koho natsional'noho universytetu, pp. 121—127.

18. Tkachuk, T. (2017), "Modern threats to information security of the state: theoretical and legal analysis", Pidpryiemnytstvo, hospodarstvo i pravo, vol 10, pp. 182—186.

19. Tkachuk, T. Yu. (2017), "Mechanisms of countering informational threats from external sources", VISNYK NTUU "KPI". Politolohiia. Sotsiolohiia. Pravo, vol. 1/2, pp. 242—254.

20. Chmyr, Ya. (2022), "Current problems of information security of Ukraine and prospective directions of their solution", Naukovi pratsi Mizhrehional'noi akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia, vol. 2 (62), pp. 149—154.

21. Shtel'makh, O. V. (2015), "Organizational aspects of countering informational aggression as a component of hybrid warfare", Aktual'ni problemy upravlinnia derzhavnoiu bezpekoiu. Naukovo-praktychna konferentsiya [Actual problems of state security management. Scientific and practical conference], Tsentr navch., nauk, ta period, vydan' NA SB Ukrainy, Kyiv, Ukraine, pp. 393—396.

Стаття надійшла до редакції 08.09.2023 р.