МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного управління та національної безпеки
Кафедра економічної теорії, інтелектуальної власності та публічного управління

Кваліфікаційна робота
на правах рукопису

**НІКОЛАЙЧУК ІВАН ДМИТРОВИЧ**
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК: 329.09.5
(індекс)

**КВАЛІФІКАЦІЙНА РОБОТА**

# ІНФОРМАЦІЙНА БЕЗПЕКА У СФЕРІ ОБОРОНИ УКРАЇНИ

(тема роботи)

281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр
кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ І. Д. НІКОЛАЙЧУК
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи:
**ЗАХАРІНА Оксана Володимирівна**
(прізвище, ім'я, по батькові)

кандидат економічних наук, доцент
(науковий ступінь, вчене звання)

Житомир – 2022

**Висновок кафедри** економічної теорії, інтелектуальної власності та публічного управління
за результатами попереднього захисту: **Ніколайчука Івана Дмитровича** допущено до захисту.

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № ____ від «____» грудня 2022 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління
к.е.н., професор _____ Валентина ЯКОБЧУК
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

«___» грудня 2022 р.

## Результати захисту кваліфікаційної роботи

Здобувач вищої освіти **Ніколайчук Іван Дмитрович** захистив
(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:
сума балів за 100-бальною шкалою _____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК
_____-_____ _____ Настасія ПУГАЧОВА
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

## АНОТАЦІЯ

НІКОЛАЙЧУК І. Д. Інформаційна безпека у сфері оборони України. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 281 «Публічне управління та адміністрування» – Поліський національний університет, Житомир, 2022.

Інформатизація є характерною особливістю сучасного суспільства, обумовлена його активною розробкою і впровадженням в усі основні сфери людської діяльності інформаційних технологій і засобів. Інформаційні ресурси та інформація все глибше проникають в наше повсякденне життя і стають одним з найголовніших факторів розвитку особистості, держави і суспільства, підвищуючи роль інформатизації. Найширші можливості, що надаються нам завдяки комп'ютерам та інформаційним технологіям, дозволяють зробити процеси моніторингу та управління державними, соціальними, економічними, оборонними та іншими об'єктами і більш автоматизованими системами, а також отримувати, зберігати, обробляти, накопичувати та передавати інформацію про всі процеси практично з будь-якою необхідною швидкістю і в будь-якій необхідній кількості.

Вивчається проблема інформаційної безпеки в Україні та захисту національного інформаційного простору від негативної пропаганди та маніпулятивних інформаційних і психологічних впливів. Проаналізовано теоретичні підходи до визначення сутності концепції інформаційної безпеки у сфері воєнної безпеки; види реальних та потенційних інформаційних загроз для медійного простору України є предметом ретельного вивчення, практичних рекомендацій щодо вдосконалення державної інформаційної політики та створення системи інформаційної безпеки.

*Ключові слова: інформаційна безпека, сфера оборони, державна політика, медіа-простір, пропаганда, державне управління, кібербезпека.*

## SUMMARY

NIKOLAICHUK I. – Information security in the field of defense of Ukraine. Qualification work on manuscript rights.

Qualification work for obtaining a master's degree in specialty 281 «Public management and administration» – Polissya National University, Zhytomyr, 2022.

Informatization is a characteristic feature of modern society, due to its active development and implementation of information technologies and tools in all major spheres of human activity. Information resources and information are increasingly penetrating our daily lives and are becoming one of the main factors in the development of the individual, the state and society, increasing the role of informatization. The widest opportunities provided to us by computers and information technologies allow us to make the processes of monitoring and managing state, social, economic, defense and other objects and more automated systems, as well as to receive, store, accumulate, process and transmit information about these processes at almost any necessary speed and in any required amount.

The article examines the problem of information security in Ukraine and the protection of the National information space from negative propaganda and manipulative information and psychological influences. Theoretical approaches to determining the essence of the concept of information security in the field of military security are analyzed; types of real and potential information threats to the media space of Ukraine are the subject of careful study, practical recommendations for improving the state Information Policy and creating an information security system.

Keywords: information security, defense, state policy, media space, propaganda, public administration, cybersecurity.

# ЗМІСТ

# ВСТУП

***Актуальність теми дослідження.*** В сучасних умовах інформаційна боротьба є найважливішою, та іноді навіть основною формою вирішення суперечок, які виникають між державами, в такій боротьбі значну кількість існуючих проблем та з метою досягнення стратегічних цілей можна досягти шляхом проведення інформаційних операцій.

На сучасному етапі у певних суб'єктів, що включають коаліції, держави, організації та особистостей, виникає егоїстичне прагнення одноосібно розпоряджатися інформаційними ресурсами, технологіями і засобами та використовувати їх для задоволення всіх суспільних інтересів та протидії інтересам імовірних конкурентів в комерційному, економічному та навіть військовому протиборстві. Інформаційні технології та інформація в даному аспекті починають виступати в якості об'єктів загроз, що створює проблему інформаційної безпеки.

В таких умовах хронічного інформаційного протистояння в країні та світі швидко зростає рівень та значно розширюється спектр інформаційних загроз. Така ситуація становить серйозну небезпеку національній і міжнародній безпеці та призводить до важкопрогнозованих і часом непередбачуваних наслідків у воєнно-політичній, економічній, військово-технічній, екологічній та інформаційній сферах. Особливо в сучасних умовах військової агресії, активних бойових дій досить значне місце займає саме інформаційна безпека.

Україна займає досить цікаве геополітичне положення та зважаючи на наявне воєнно-політичне становище також існує доволі розвинута інформаційна інфраструктура, просто не можливо залишатись осторонь від сьогочасних світових тенденцій, постійно перебуваючи під потужним зарубіжним інформаційним впливом. Зовнішній негативний інформаційний вплив має системний та цілеспрямований характер, що як наслідок зумовлює появи загроз національній безпеці України, саме в інформаційній сфері, що в свою чергу завдає державі помітних збитків.

Головним чином це стосується і виконання завдань щодо оборони країни, адже саме ця діяльність напряму спрямована на захист національних інтересів держави від зовнішніх загроз, що пов’язані з підготовкою та раціональним веденням війни з припустимим агресором.

Проблеми та шляхи інформаційного забезпечення безпеки держави не є новітніми з точки зору дослідницького питання. Вони активно розглядаються в роботах вітчизняних і зарубіжних авторів в контексті тих чи інших наукових інтересів. Інформаційну безпеку, головним чином, як проблеми захисту сучасного національного інформаційного простору розглядали чимало науковців. Таких, як Б. Кормича, А. Марущака, В. Почепцова, В. Ліпкана, В. Петрика та інших спеціалістів. Зокрема проблеми забезпечення кібернетичної безпеки вивчали В. Бурячок, Р. Лук’янчук, В. Гавловский, В. Шеломенцев Д. Дубов, М. Погорецький, В. Номоконов, А. Бабенко та інші науковці. Проте у працях цих науковців інформаційна безпека вивчалась, виключно, як складову національної безпеки, лише як невід’ємний компонент.

Таким чином, тема вивчення сутності та змісту інформаційної безпеки в сучасних умовах дуже актуальна. Особливою ця тематика стала в світлі глобальних геополітичних тенденцій останніх місяців в умовах війни не лише на полі бою, але й у інформаційному полі.

*Метою дослідження* є комплексне вивчення та визначення особливостей забезпечення інформаційної безпеки в системі національної безпеки та оборони країни. Ланцюг дослідження передбачає вирішення наступних завдань:

- розглянути основні категорії інформаційної безпеки;

- охарактеризувати сутність інформаційної безпеки як найважливішого компонента національної безпеки;

- дослідити поняття і зміст інформаційної безпеки України;

- проаналізувати особливості оцінки стану та організації захисту від інформаційних загроз в Україні.

*Об'єктом дослідження*: виступає інформаційна безпека в сфері оборони держави.

*Предмет дослідження*: стан і методи забезпечення інформаційної безпеки в сфері оборони України в сучасних умовах.

*Методи дослідження.* Головними методологічними засадами роботи стало використання загальнонаукових та спеціальних, теоретичних та емпіричних, методів дослідження, таких як: теоретико-методологічний аналіз щоб визначити актуальний стану нормативно-правової бази у сфері державного контролю інформаційною безпекою; психодіагностичні методи щоб встановити як інформаційне поле впливає на свідомість суспільства та психоемоційний стан людей; аналіз статистичної та емпіричної інформації – щоб визначити тенденції щодо змін у державно-суспільних відносинах та актуальних напрямах підвищення дієвості державного управління. Методи, що використовувались дали можливість встановити пріоритетні управлінські рішення та підготувати рекомендації по оптимізації діяльності забезпечення інформаційної безпеки у сфері оборони України.

*Перелік публікацій автора за темою дослідження.* Основні результати дослідження оприлюднені в трьох публікаціях тез на міжнародних конференціях.

*Практичне значення отриманих результатів.* Полягає в тому, що розроблено теоретичні положення доведені до рівня конкретних практичних пропозицій щодо удосконалення діяльності та підвищення ефективності системи забезпечення національної безпеки у сфері оборони України.

*Структура та обсяг роботи.* Випускна кваліфікаційна робота містить вступ, три розділи основної частини та висновки до них, висновки та пропозицій, список використаних джерел. Основний текст роботи викладено на 32 сторінках. Список використаних джерел включає 33 найменування.

# РОЗДІЛ 1.
# ТЕОРЕТИЧНІ АСПЕКТИ ВИВЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СФЕРІ ОБОРОНИ ДЕРЖАВИ

Стрімкий розвиток і широке застосування інформаційних технологій, як у повсякденному житті, так і управлінні державою є основним фактором оригінальності сучасного етапу економічного і науково-технічного прогресу. Інформація та інформаційні технології все більше стають частиною суспільства і визначають його розвиток, а також служать новими предметами загальнонаціональної могутності. Становлення і розвиток сучасного інформаційного суспільства радикально змінює багато аспектів життєдіяльності людини, зачіпаючи політичну, військову, екологічну та соціальну сфери. У цих умовах інформаційного суспільства змінює предмет основної праці на інформацію і знання. У сучасних реаліях фундаментальною основою глобалізації стає впровадження інформаційних систем різних держав до єдиної глобальної інформаційної системи, формування єдиного інформаційного простору, створення Всесвітніх інформаційно-телекомунікаційних мереж, а також впровадження новітніх інформаційних технологій до всіх галузей суспільного життя, включаючи і забезпечення економічної безпеки держави.

Процес глобальної інформатизації суспільства охопив практично всі країни світу і зараз є основою науково-технічного та соціально-економічного розвитку. Інформатизація, в своїй основі, є організаційним соціально-економічним і науково-технічним процесом створення і забезпечення комфортабельних факторів для багатогранного задоволення потреб в інформаційних ресурсах і реалізації прав громадян, органів державної влади та управління, що ґрунтуються на формуванні та використанні інформаційних ресурсів і експлуатування інформаційних систем, мереж, ресурсів та інформаційних технологій, використовуючи обчислювальну і комунікаційну техніку.

Виділяють наступні основні завдання інформатизації:

- багатогранне забезпечення інформаційних потреб суб'єктів інформаційних відносин;
- створення глобального інформаційного простору, що забезпечує інформаційну безпеку;
- створення, впровадження та експлуатування інформаційних систем, інформаційних технологій та інформаційних продуктів загального значення;
- підготовка персоналу та проведення організаційних заходів у сфері підвищення їх інформатизаційної кваліфікації [5].

Осягнення сутності значення поняття «інформаційна безпека» є головним завданням наукового аналізу. Кожне вчення лише тоді досягає наукової зрілості та досконалості, коли розкриває саму сутність досліджуваних явищ, маючи можливість прогнозувати прийдешні зміни не тільки в сфері явищ, а й у сфері сутностей.

Концептуальні та науково-методологічні засади інформаційної безпеки знаходяться тільки на стадії розробки. Створюючи теорії інформаційної безпеки основоположним завданням слід вважати формування понятійного апарату. Фундаментальними поняттями є інформаційна загроза, інформаційна небезпека та інформаційна безпека.

Виділяють два можливих тлумачення поняття «інформаційна небезпека»:

В першу чергу, як стан навколишнього середовища або об'єкта, в якому є потенційна можливість заподіяти їм суттєвої шкоди або шкоди напрямом надання впливу на інформаційну сферу об'єкта, а також як властивість об'єкта, яке характеризується здатністю спричинити суттєвої шкоди іншому об'єкту через впливу на його інформаційну сферу [6].

Виходячи з усього, можна висловити поняття інформаційної безпеки, яке визначає її як стан об'єкта, коли йому через вплив на його інформаційну сферу не може бути завдано суттєвої шкоди, або така властивість об'єкта, що визначає його здатність не завдавати істотної шкоди будь-якому об'єкту шляхом надання впливу на інформаційну сферу цього об'єкта.

Інформаційна загроза – це загроза об'єкту шляхом надання згубного або

протизаконного впливу на його інформаційну сферу:

- намір заподіяти (завдати) об'єкту суттєвої шкоди шляхом надання впливу на його інформаційну сферу;
- інформаційна небезпека, реалізація якої стає досить ймовірною;
- фактор або сукупність факторів, що створюють конкретну інформаційну небезпеку об'єкту; подібними факторами можуть бути дії, поведінка об'єктів, природні явища і т. д [10].

Все вищесказане дозволяє сформулювати інше поняття інформаційної безпеки, яке визначає її як такий стан країни, в якому громадянам, об'єднанням і громадським групам осіб, державі та суспільству не може бути завдано суттєвої шкоди шляхом нанесення згубного впливу на її інформаційну сферу.

Головними об'єктами інформаційної безпеки є права і свободи особистості, матеріальні і духовні цінності суспільства і конституційний лад держави, його суверенітет, територіальна цілісність, економіка, військова справа та інші сфери державної діяльності.

Особистість – осередок суспільства, це фундаментальний елемент. Без особистості не може існувати суспільства, але і особистість поза суспільством бути не може. Основним зобов'язанням держави є забезпечення умови існування і особистості, і суспільства. Держави, потреба в яких відсутня у особистості і суспільства, не можуть існувати довго і з часом зникають зі світової арени. Головною умовою сталого розвитку взаємин між особистістю, суспільством і державою виступає баланс їх взаємин [15].

Інформаційна безпека особистості – це такий стан людини, при якому його особистості не може бути завдано будь-якої істотної шкоди, завданий впливом на навколишній інформаційний простір.

У процесі сучасної інформатизації людина стала дуже інформаційно «прозорою». За наявності коштів та бажання будь-яка інформація, котрою володіє людина про конкретну особу може стати доступною та може бути використана в корисливих цілях іншою людною, групою осіб, громадською групою або державою. Лише незначна частина населення має можливість

запобігти небажаному доступу до своєї інформації. Велика частина громадян такої можливості не мають та залишаються абсолютно беззахисними в цьому плані, наражаючи свою конфіденційність на небезпеку.

Інформаційна безпека суспільства – це стан такий суспільства, за якого йому не може бути завдано суттєвої шкоди шляхом впливу на його інформаційну сферу. В її основу входить безпека індивідуальної, групової та масової свідомості суспільства при наявності інформаційних загроз, до яких в перш за все варто віднести інформаційно-психологічний вплив. Вплив таких загроз може викликати соціально-психологічну та психоемоційну напруженість, морально-політичну дезорієнтацію, спотворення моральних критеріїв і норм, і, як наслідок, неадекватну поведінку окремих осіб, груп та мас людей. В результаті таких впливів можливі глибокі трансформації індивідуальної, групової і масової свідомості, негативні зміни морально-політичного і соціально-психологічного клімату в суспільстві [14].

Інформаційна безпека держави – це такий стан держави, за якого йому не може бути завдано суттєвої шкоди шляхом надання впливу на його інформаційну сферу. Саме забезпечення інформаційної безпеки держави на пряму пов'язане із забезпеченням національної безпеки.

Нові реалії сучасності вимагають нового підходу до питань економічної безпеки, в яких інформаційна безпека починає відігравати все більш важливу роль. Такі тенденції інтенсивно розвиваються з 80х рр. минулого століття і викликані науково-технічним прогресом у сфері інформаційних технологій, глобальних систем телекомунікацій, засобів зв'язку. У цей період з'явилися ефективні технічні засоби обміну цифровою інформацією, які могли б забезпечити інформаційне та телекомунікаційне з'єднання різних регіонів світу з глобальною економічною системою [18].

В даний час розвиток військової техніки і технологій призвело до практичної неможливості ведення війни у великих масштабах. Основною зброєю в XXI ст. стають все більшою мірою економічні і, перш за все, фінансові методи. Багато країн світу не мають свого конкурентоспроможного

науково-технічного потенціалу і повністю залежать від техніки і технології розвинених країн.

Практика 90-х рр. минулого століття і нульових років нинішнього століття показала високу ефективність інформаційно-фінансового впливу на національні економіки, яке дозволяє вирішувати політичні завдання без ведення бойових дій.

Економічна та інформаційна глобалізація світових відносин супроводжується створенням ефективних механізмів і засобів для інформаційного та фінансового впливу на партнерів і конкурентів у місцевому, регіональному та глобальному масштабі. Мета такого впливу, як правило, полягає в зміні розподілу реальних благ, вироблених на користь тих, хто розробляє, має і застосовує відповідні технології. Сучасна ситуація вимагає більшої уваги до захисту інтересів держави від нових реальних і потенційних загроз, забезпечення інформаційної та економічної безпеки. У сучасній ситуації, враховуючи зростаючу проблему взаємозв'язку інформаційної та економічної безпеки, дуже важливо своєчасно виявляти і оцінювати виникаючі загрози економічної та інформаційної безпеки, і на цій підставі вживати необхідних заходів щодо запобігання загрозам, захисту інформації та економічних інтересів від потенційних джерел небезпеки. Загрози економічної та інформаційної безпеки можуть бути спрямовані як на руйнування будь-якого компонента системи забезпечення національної безпеки та їх взаємозв'язку, так і на механізм забезпечення в цілому. Інформаційні загрози економічної безпеки мають різний характер, закінчуються з систем зв'язку і телекомунікацій, можуть бути глобальними за своїми масштабами (такі прийнято називати викликами), регіональними, тобто відносяться до певного регіону, групі країн, або загрози національні, тобто виникають в самій країні.

У сучасних умовах економічні загрози, як правило, мають довгостроковий характер і спрямовані на руйнування економічного потенціалу країни, її життєзабезпечуючих сфер. Вплив загроз в інформаційній сфері у всезростаючій мірі направлено на інтереси економіки, суспільства і держави.

При цьому неухильно зростає інформаційний вплив на економічну систему, включаючи її фінансову сферу (наприклад, інформаційні атаки проти національних валют і фондових ринків, що прокотилися по світу в кінці 90-х рр.), фондові ринки з грою на зниження капіталізації підприємств, а потім їх скупкою за нижчою ціною, в поєднанні з поширенням інформації щодо створення негативного образу конкурента і т. д. (наприклад, в період світової фінансової кризи, особливо 2008-2009 рр.) [13].

Таким чином, нові виклики і загрози (перш за все міжнародний кібертероризм, інформаційне шпигунство, організована злочинність в інформаційній сфері, небезпека поширення вірусних комп'ютерних атак на інформаційно-керуючі системи в економіці і, перш за все, у фінансовій сфері тощо) носять глобальний характер і вимагають адекватної відповіді з боку всього міжнародного співтовариства і солідарних зусиль для їх подолання. В даний час істотно зростає роль інформаційної безпеки національної економіки, все більш актуальною стає проблема боротьби з кіберзлочинністю у фінансовій сфері.

# РОЗДІЛ 2.
# АНАЛІЗ ДІЮЧОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СФЕРІ ОБОРОНИ УКРАЇНІ

З початком збройної агресії проти України, країна-агресор активізувала інформаційну війну, що в свою чергу викликала загрозу інформаційній безпеці. Значна кількість антиукраїнської пропаганди, постановочні новинні сюжети, відверті фейки, які поширюють російські медіа та соцмережі, і як наслідок це не лише погіршення ставлення жителів Донбасу та росіян, але й на деяких представників всесвітнього співтовариства. Оскільки такі інформаційні атаки ворога фінансуються за рахунок державних коштів, вони набувають все більш глобального характеру. Ось лише у 2016 р. міжнародно-трансльований телеканал Russia Today (RT), котрий розповсюджує інформацію кількома мовами: арабською, англійською та іспанською, одержав фінансування у сумі 19 млрд рублів (307 млн дол. США), в той час коли для державних російських ЗМІ було виділено 80,2 млрд р., що на 30 % більше відносно до 2015 р. Також, у Росії створено кілька науково-дослідних центрів, завданням яких є ведення інформаційної діяльності на територіях колишніх республік бувшого Радянського Союзу, зокрема і в Україні [26].

Так, 22 лютого 2017 р. Міноборони РФ було оголошено про створення спеціальних військ для інформаційних операцій. В реальності це не було створення нових, а лише легалізація існуючих підрозділів, які досить тривалий час та успішно здійснюють інформаційні та кібератаки. Ще в 2007 р. цими військами було атаковано Естонію. Також здійснювались атаки на електронну пошту держсекретаря США та з подальшим використання добутої інформації на виборах – це можна вважати елементом гібридної війни, яку Російська Федерація веде у США на протязі багатьох років [26].

Новий етап технологічної революції в інформаційній сфері, пережитий світом на даному етапі, передбачає серйозні зміни в суспільстві в цілому. Змінюється стиль життя мільйонів і мільйонів людей. Процеси глобалізації

зачіпають все нові і нові сфери діяльності. Це стає актуальним і в сфері забезпечення безпеки України. У цій сфері чітко виділяється специфіка забезпечення інформаційної безпеки. Вона знайшла своє відображення в доктрині інформаційної безпеки України, затвердженій Указом Президента України від 28 квітня 2014 р. [29].

У доктрині, що є офіційним документом, вперше дана офіційна оцінка значущості і системної сутності інформації: «сучасний етап розвитку суспільства визначається зростаючою роллю інформаційної сфери, що являє собою всю сукупність інформації. Інформаційна сфера, будучи системоутворюючим фактором існування суспільства, активно впливає на стан економічної, оборонної, політичної, та інших складових безпеки України. Саме під інформаційною безпекою України і розуміється такий стан захищеності її національних інтересів в інформаційній сфері, що і визначаються сукупністю відносно збалансованих інтересів індивіда, суспільства та держави» [29].

Указом Президента України «Про Доктрину інформаційної безпеки України» від 8 липня 2009 року № 514, який втратив чинність згідно з Указом від 6 червня 2014 року № 504/2014 [29], основу становить Закон України «Про основи національної безпеки України» [21] та в повному обсязі відповідає його структурі, яка розподілила усі сфери функціонування та життєдіяльності держави на: сферу державної безпеки; зовнішньополітичну; воєнну; економічну; внутрішньополітичну; гуманітарну та соціальну сфери; екологічну та науково-технологічну сфери. Але сам Указ не до кінця відображав дані положення згаданого закону як виключно декларативного документу, оскільки кінцеві положення відповідали виключно політичним амбіціям тодішнього керівництва держави, і на жаль не реально існуючим потребам сучасного суспільства.

У загальних положеннях даного указу цілком обґрунтовано зазначалося, що саме інформаційна безпека є невідривною складовою всіх сфер національної безпеки країни. Одночасно інформаційна безпека є головною і самостійною сферою, яка забезпечує національну безпеку. Завдяки чому

розвиток України як демократичної, суверенної, економічно стабільної та правової держави припустимий лише за умови досягнення та постійного забезпечення відповідного рівня інформаційної безпеки держави.

У прикінцевих положеннях згаданої Доктрини головним рахувалося необхідність сформувати державну політику щодо інформаційної безпеки України та розробити ряд проєктів концепцій, цільових програм, стратегій та планів дій щодо забезпечення інформаційної безпеки України. Проте положення щодо підготовки конкретних пропозицій для подальшого *системного вдосконалення* методичного, правового, організаційного та науково-технічного забезпечення інформаційної безпеки України, в першу чергу викликало значне непорозуміння та занепокоєння.

«Положення про Міністерство інформаційної політики України» яке було прийнято постановою Кабінету Міністрів України від 14 січня 2015 р. № 2 «Питання діяльності Міністерства інформаційної політики України» [22], має суто політичний характер покликаний протидіяти інформаційній російській пропаганді в умовах воєнного конфлікту на території нашої країни і абсолютно не враховує існування багатоманіття інформаційної політики України.

Указ Президента України від 26 травня 2015 року № 287/2015 «Про Стратегію національної безпеки України» [28] є другорядним відповідно до закону. Ця Стратегія була спрямована на реалізацію до 2020 року вказаних цією Стратегії пріоритетів державної політики національної безпеки та проведення реформ, які були передбачених Угодою про асоціацію між Україною та ЄС [25], але не суперечить закону України. Тому що визначені цілі цієї стратегії та шляхи їх реалізації аніяким чином не відсвічуються структурою доктрини інформаційної безпеки держави.

Серед важливих загроз національній безпеці України навіть не згадуються загрози інформаційній безпеці, таких, як формування російськими ЗМІ протилежної до дійсності викривленої інформаційної картини світу, приниження української мови і культури, інформаційно-психологічна війна, фальшування української історії. Також досить побічно згадуються загрози які

стосуються кібербезпеки і лише, що стосується безпеки інформаційних ресурсів: уразливість об’єктів інфраструктури, більшості державних інформаційних ресурсів до кібератак; матеріальна та моральна застарілість систем охорони державної таємниці та інших видів інформації, що мають обмежений доступ тощо. На нашу думку все має бути навпаки.

Поняття інформаційної безпеки України розкривається як стан захисту національних інтересів країни в інформаційній сфері, яку визначає сукупність збалансованих особистісних інтересів, інтересів суспільства і держави. Інформаційна сфера являє собою сукупність інформаційних ресурсів та інформаційної інфраструктури об'єкта захисту. Інформаційний ресурс – це сукупність збереженої, оброблюваної і переданої інформації, використовуваної для забезпечення різних процесів управління [23].

До інформаційних ресурсів відносяться:

- інформаційні ресурси підприємств оборонно-промислового комплексу, в зберіганні яких знаходяться відомості про ключові напрямки розвитку озброєння, про науково-технічний і виробничий потенціал, про обсяги поставок і запаси стратегічних видів ресурсів;
- інформаційне забезпечення управлінських систем і систем зв'язку;
- інформація про фундаментальні та прикладні НДР, що мають державне значення та ін.;
- інформаційна інфраструктура – це сукупність інформаційних підсистем, центрів управління, апаратно-програмних засобів і технологій забезпечення збору, зберігання, обробки і передачі інформації [23].

Інформаційна інфраструктура включає: інформаційну інфраструктуру центральних, місцевих органів державного управління, а також науково-дослідних установ; інформаційну інфраструктуру підприємств оборонно-промислового комплексу та науково-дослідних установ, що виконують державні оборонні замовлення, або займаються оборонною проблематикою; програмно-технічні засоби автоматизованих і автоматичних систем управління і зв'язку.

Під загрозою безпеки інформації розуміється сукупність умов і факторів, що створюють потенційну або реально сучасну небезпеку, що пов'язана з витоком інформації і (або) несанкціонованими і (або) ненавмисними впливами на неї. Загрози інформаційної безпеки Російської Федерації поділяються на зовнішні і внутрішні [14].

Оцінка стану інформаційної безпеки ґрунтується на доскональному аналізі джерел загроз, а також потенційної можливості порушення захисту. Діяльність, спрямовану на запобігання витоку інформації, що захищається від ненавмисних та несанкціонованих впливів на неї, називають захистом інформації. Об'єктом захисту є інформація або носій інформації, або інформаційний процес, які потрібно захищати.

Захист інформації організовується за трьома основними напрямками: від витоку ресурсів, від несанкціонованого впливу і від ненавмисного впливу (рис. 2.1.).

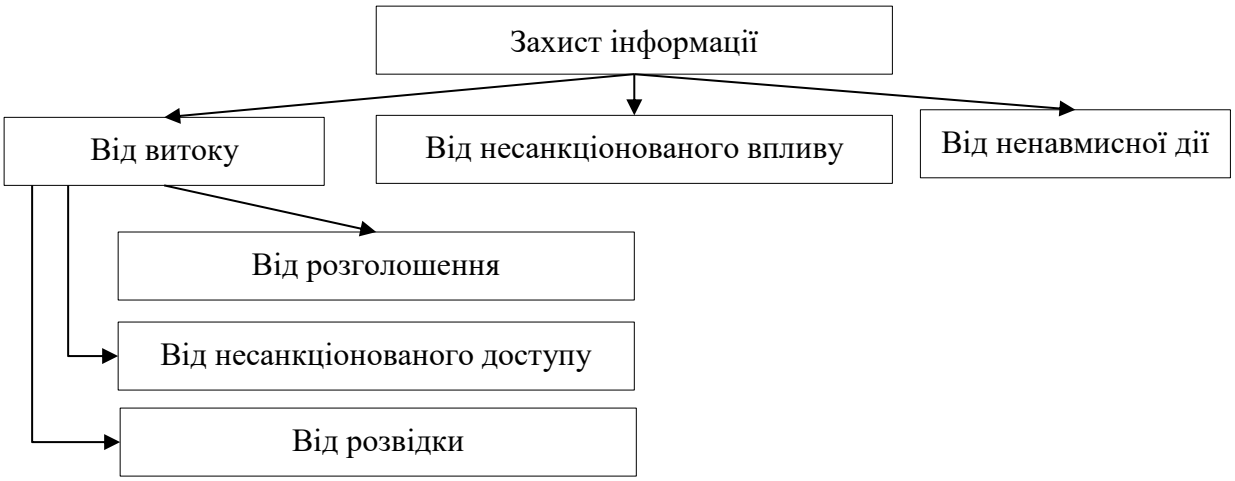



**Рис. 2.1. Напрямки захисту інформації**

Сучасний соціально-економічний розвиток України нерозривно пов'язаний із загостренням проблеми забезпечення її економічної безпеки, розширенням масштабів економічних загроз і появою нових форм і видів економічної злочинності. У контексті розглянутого питання до нових видів загроз кінця XX-го початку XXI-го ст. можна віднести і блок інформаційних загроз. Інформаційна сфера, будучи фактором прогресу, одночасно виступає і

як специфічний носій загроз економічній безпеці країни.

Технології постійно розвиваються, і нові кіберзагрози продовжують створюватися. В рамках технологічного прогресу кібербезпека повинна бути невід'ємною і нероздільною частиною самого прогресу. На жаль, кібербезпека поки не входить в число ключових факторів національної та промислової технологічної стратегії великого числа країн. Керівництво країн має усвідомлювати свій поточний рівень компетенцій у сфері кібербезпеки і в той же час виявляти області, де контроль кібербезпеки вимагає посилення. Глобальний індекс кібербезпеки – ДВК) – це показник рівня розвитку кібербезпеки конкретної країни. ДВК спрямований на створення для країн правильної мотивації, щоб інтенсифікувати їхні зусилля у сфері кібербезпеки. Кінцева мета – допомогти в розвитку глобальної культури кібербезпеки та її інтеграції в найважливіші інформаційні та комунікаційні технології.

Глобальний індекс кібербезпеки, ДВК – Global Cybersecurity Index, GCI) – це показник рівня розвитку кібербезпеки конкретної країни, який спрямований на створення для країн правильної мотивації, щоб інтенсифікувати їх зусилля у сфері кібербезпеки. Кінцева мета – допомогти у розвитку глобальної культури кібербезпеки та її інтеграції найважливіші інформаційні та комунікаційні технології [25].

Створений на основі глобальної програми кібербезпеки Міжнародного союзу електрозв'язку, ДВК оцінює рівень зобов'язань у п'яти сферах: правові заходи, технічні заходи, організаційні заходи, розвиток потенціалу та міжнародне співробітництво. Результатом став Індекс на рівні окремих країн і глобальний рейтинг готовності системи кібербезпеки. ДВК прагне визначити ефективність або успішність не конкретної міри, а існуючих і діючих національних структур, відповідальних за кібербезпеку.

Кібербезпека має першорядне значення для підтримки технологічно безпечної моделі. Перебої в подачі електроенергії або порушення роботи фінансових систем через втручання в роботу мереж ІКТ стали реальністю і становлять загрозу національній безпеці. Існують численні і організовані

шкідливі онлайн-агенти, що переслідують найрізноманітніші цілі: політичні, злочинні, терористичні та хакерські. З часом і в міру накопичення досвіду наявні в їх розпорядженні кошти стають більш витонченими і складними; зростаюче число взаємопов'язаних платформ сприяє появі нових напрямків атак. Зворотного шляху в більш прості часи просто немає. В рамках технологічного прогресу кібербезпека повинна бути невід'ємною і нероздільною частиною самого прогресу. У сучасному цифровому світі кіберзлочинність є ключовою загрозою зростання світової економіки. Метою ДВК є створення загальної картини того, на якому рівні країни перебувають у справі забезпечення національної кібербезпеки. Стратегічне бачення ABI Research і MCE-просування обізнаності про кібербезпеку і важливої ролі урядів-має відігравати важливу роль в об'єднанні відповідних механізмів, спрямованих на підтримку і просування цієї найважливішої дисципліни. Захист єдиного кіберпростору повинен включати розвиток кібербезпеки.

Ці п'ять показників відіграють особливу роль в оцінці потенціалу кібербезпеки держав, оскільки вони формують характерні ключові компоненти будь-якої національної культури. Кібербезпека є сферою діяльності, яка проходить через всі галузі і сектори як вертикально, так і горизонтально. Отже, забезпечення можливості розвитку потенціалу держав вимагає вкладень з боку політичних, економічних і соціальних сил. Над цим можуть працювати правоохоронні органи, органи юстиції, навчальні заклади та Міністерства, оператори з приватного сектора, розробники технологій, партнерства держави і приватного сектора, а також міждержавні співпраці [25].

*Правові заходи.* Законодавство є найважливішим засобом для створення гармонійної структури, в рамках якої всі організації повинні адаптуватися під єдину нормативно-правову базу, що може бути забезпечено як за допомогою заборони певної злочинної діяльності, так і за рахунок встановлення мінімальних регулюючих вимог. Правові заходи також дозволяють країнам встановлювати основні механізми реагування на порушення: шляхом розслідування і покарання злочинів і застосування санкцій у разі недотримання

або порушення закону. В рамках законодавчої бази встановлюються мінімальні стандарти поведінки у всіх аспектах, застосовні до всіх і є основою для нарощування потенціалу кібербезпеки. Зрештою, мета полягає в тому, щоб дати всім країнам можливість розробити відповідне законодавство, що сприяє гармонізації практик роботи на наднаціональному рівні і створенню умов для введення заходів, що забезпечують взаємодію і допомагають у веденні міжнародної боротьби з кіберзлочинністю. Оцінка правового середовища може виконуватися виходячи з існування і числа правових інститутів і програм у сфері кібербезпеки і боротьби з кіберзлочинністю.

*Технічні заходи.* Технології – це перший засіб захисту від кіберзагроз і шкідливих онлайн-агентів. Без застосування належних технічних заходів і можливостей виявляти кібератаки і реагувати на них країни і знаходяться в них організації залишаються вразливі для кібератак. Поява і ефективний розвиток ІКТ можливі лише в умовах довіри і безпеки. Тому країнам необхідно розробляти стратегії для встановлення мінімальних прийнятних критеріїв безпеки та запровадження схем акредитації програмних додатків і систем. Поряд з цим повинна бути створена загальнонаціональна організація, що реагує на кіберінциденти на національному рівні, принаймні, в рамках відповідного урядового органу, а також розроблена національна програма зі спостереження, попередження та реагування на інциденти. Оцінка технічних заходів може виконуватися виходячи з існування і числа технічних установ і програм у сфері кібербезпеки, затверджених або створених державою.

*Організаційні заходи.* Організаційні та процедурні заходи необхідні для належної реалізації державних ініціатив будь-якого типу. Кожна держава повинна встановити широкі стратегічні цілі, а також розробити всебічний план їх впровадження, реалізації та контролю. Для втілення стратегії в життя і оцінки успіху або невдачі реалізації плану повинні бути створені такі структури, як державні органи. Без державної стратегії, моделі управління та контрольного органу діяльність у різних секторах і галузях стає роз'єднаною і розрізненою, що перешкоджає досягненню гармонізації на державному рівні у

сфері розвитку потенціалу кібербезпеки.

*Створення потенціалу.* Створення потенціалу відноситься до перших трьох заходів (правові, технічні та організаційні). Розуміння технологій, ризиків і наслідків може допомогти в розробці більш досконалого законодавства, більш досконалої політики і стратегій, а також у забезпеченні кращої організації в області різних ролей і сфер відповідальності. Кібербезпека – це відносно нова сфера діяльності, що з'явилася ненабагато пізніше появи Інтернету. Як правило, вивчення цієї сфери ведеться з точки зору технологій; однак існує безліч соціально-економічних і політичних факторів, що мають до цієї сфери саме пряме відношення. Створення трудового та інституційного потенціалу необхідно для розширення знань і розвитку ноу-хау в різних секторах, для застосування найбільш підходящих рішень і сприяння розвитку якомога більш компетентних фахівців. Програма створення потенціалу для розвитку та підвищення кібербезпеки повинна включати роботу з підвищення інформованості та забезпечення доступності ресурсів. Створення потенціалу може оцінюватися виходячи з існування і числа науково-дослідних, освітніх і навчальних програм, а також кваліфікованих професіоналів і органів державного сектора.

*Співпраця.* Забезпечення кібербезпеки вимагає вкладу всіх секторів і всіх галузей і тому має здійснюватися з використанням підходу із залученням різних зацікавлених сторін. Співпраця сприяє веденню діалогу, забезпеченню координації та створенню більш всеосяжної галузі впровадження кібербезпеки. Представникам різних секторів і операторам з приватного сектора дуже важко здійснювати обмін інформацією. І цей процес стає все більш складним на міжнародному рівні. Однак проблема кіберзлочинності має глобальний характер, і для неї не існує державних кордонів і відмінностей між різними секторами. Співпраця дає можливість обміну інформацією про загрози, сценарії атак та обміну передовими практиками у сфері реагування та захисту. Розширення ініціатив у сфері співпраці може сприяти розвитку та зміцненню потенціалу кібербезпеки, допомагати запобіганню виникненню повторних і

постійних онлайн-загроз, а також покращувати якість розслідувань, сприяти переслідуванню і затриманню шкідливих агентів. Оцінка співпраці на національному та міжнародному рівні може виконуватися виходячи з існування і числа партнерств, програм співробітництва та мереж обміну інформацією.

Індекс України в рейтингу за рівнем кібербезпеки становить 68,83 зі 100 можливих балів. У повному списку країна обігнала Японію, Південну Ізраїль та Корею. Всього в рейтингу 160 країн.

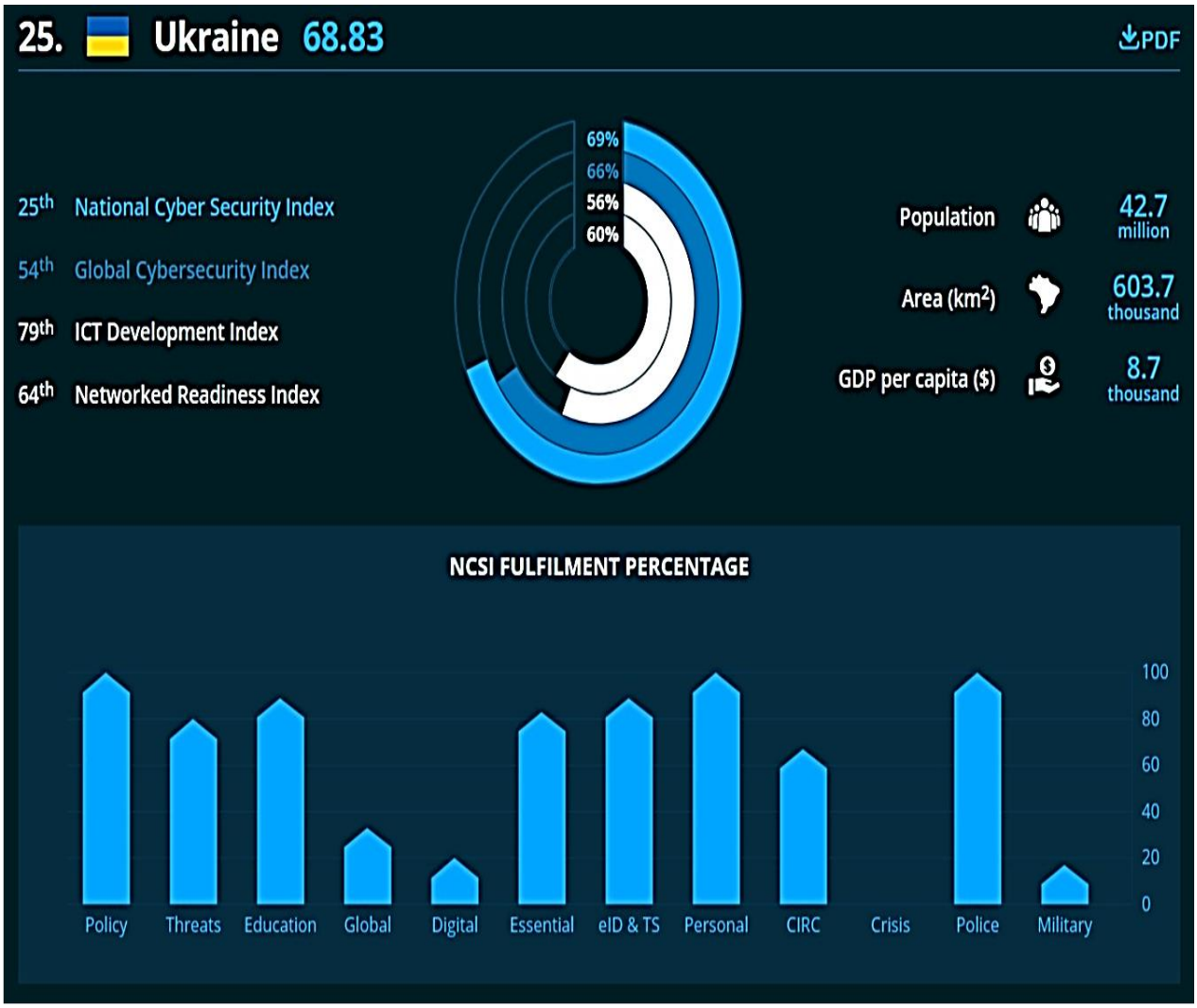
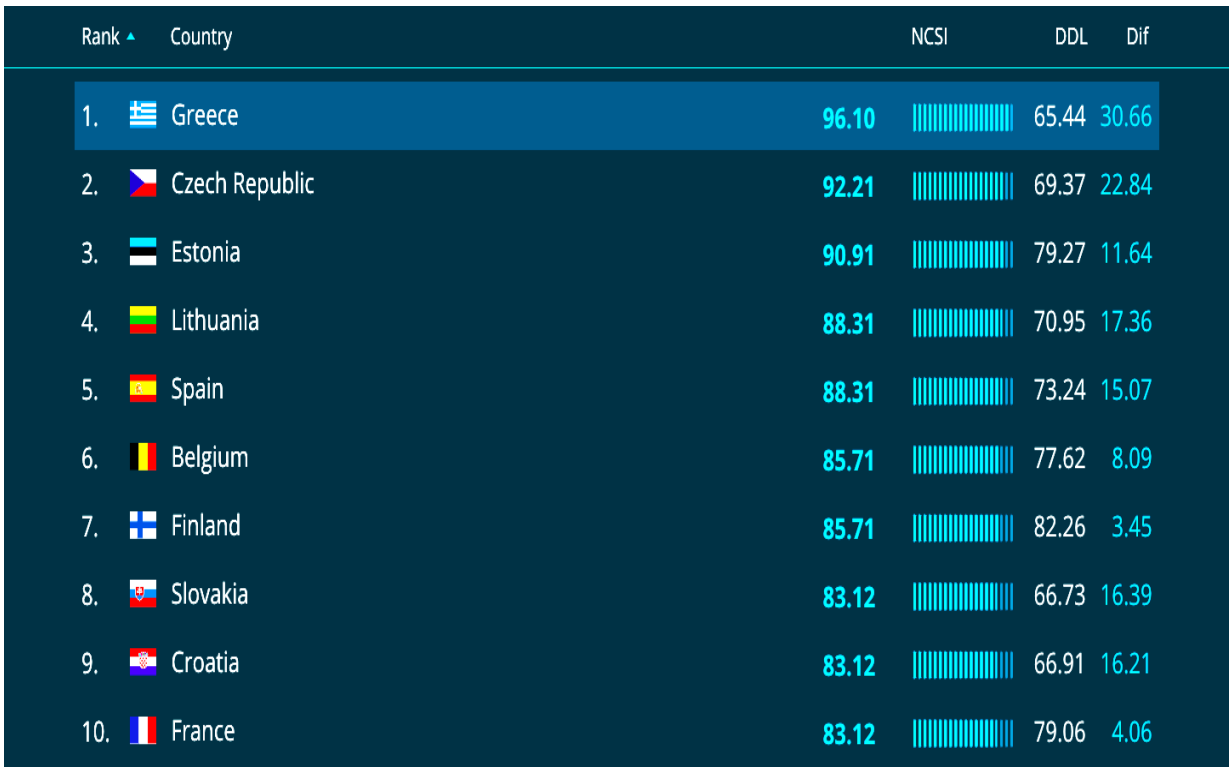



**Рис. 2.2. Індекс України в рейтингу за рівнем кібербезпеки**

Останнього разу «Державний індекс кібербезпеки» оновлювали в 2018 році. Тоді, Україна піднялася на чотири позиції. «Покращення займаних позиції України в рейтингу індексі кібербезпеки стало імовірним завдяки тому що було прийнято ряд законодавчих актів у галузі кібербезпеки та кіберзахисту» [31].



| Rank | Country | NCSI | DDL | Dif |
|---|---|---|---|---|
| 1. | Greece | 96.10 | 65.44 | 30.66 |
| 2. | Czech Republic | 92.21 | 69.37 | 22.84 |
| 3. | Estonia | 90.91 | 79.27 | 11.64 |
| 4. | Lithuania | 88.31 | 70.95 | 17.36 |
| 5. | Spain | 88.31 | 73.24 | 15.07 |
| 6. | Belgium | 85.71 | 77.62 | 8.09 |
| 7. | Finland | 85.71 | 82.26 | 3.45 |
| 8. | Slovakia | 83.12 | 66.73 | 16.39 |
| 9. | Croatia | 83.12 | 66.91 | 16.21 |
| 10. | France | 83.12 | 79.06 | 4.06 |

**Рис. 2.3. рейтинг індексів країн світу за рівнем кібербезпеки**

Даний рейтинг очолює Греція – 96,10 балів. До десятки лідерів входять Естонія, Чехія, Іспанія, Литва, Фінляндія, Бельгія, Словаччина, Хорватія та Франція. Останню сходинку займає Південний Судан [31].

Отже, можна зробити висновок що Україні нині практично відсутні ознаки політики в сфері інформаційної безпеки, хоча існує значна кількість науково-обґрунтованих та теоретико-прикладних та теорій щодо її забезпечення. Себто уряд приймає певні правові положення покладаючись виключно на своє бачення, а не теоретичними обґрунтуваннями, що як наслідок призводить до виникнення нових міністерств (заради посад та портфелів, а не для вирішення проблем) та еклектичних нормативно-правових актів.

# РОЗДІЛ 3.
# УДОСКОНАЛЕННЯ МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Державна політика в області забезпечення безпеки реалізується органами державної влади, органами місцевого самоврядування на основі Стратегії національної безпеки України, інших концептуальних і доктринальних документів, що розробляються Радою Безпеки і затверджуються указами Президента України.

Громадяни та громадські об'єднання беруть участь у реалізації державної політики в галузі забезпечення безпеки. Правову основу забезпечення безпеки складають Конституція України, загальновизнані принципи і норми міжнародного права, міжнародні договори ратифіковані Україною, конституційні закони та інші нормативно- правові акти органів місцевого самоврядування, прийняті в межах їх компетенції в галузі безпеки.

Міжнародне співробітництво України в області забезпечення безпеки здійснюється на основі загальновизнаних принципів і норм міжнародного права і міжнародних договорів України. Основними цілями міжнародного співробітництва в галузі забезпечення безпеки є:

1) захист суверенітету і територіальної цілісності України;

2) захист прав і законних інтересів українських громадян за кордоном;

3) зміцнення відносин зі стратегічними партнерами України;

4) участь у діяльності міжнародних організацій, що займаються проблемами забезпечення безпеки;

5) розвиток двосторонніх і багатосторонніх відносин з метою виконання завдань забезпечення безпеки;

6) сприяння врегулюванню конфліктів, включаючи участь у миротворчій діяльності.

Як і будь-яка інша держава, в України є цілий ряд інструментів, які вона може використовувати для досягнення своїх національних інтересів. Їх

специфічний зміст (політичний, економічний, військовий, військово-технічний, науковий, культурний, етнічний, релігійний і т.д.) залежить від ієрархії національних інтересів, співвідноситься відповідно до реальної політичної та економічної ваги, духовним потенціалом, геостратегічним становищем, напрямком і характером міжнародної діяльності, а також іншими параметрами.

З'явилася нова система міжнародних відносин, яка підтверджує пріоритет політичних, дипломатичних та інших невійськових засобів вирішення конфронтацій і конфліктів. Тим не менш, навряд чи можна вважати, що військові сили вже втратили своє значення на підтримку стабільності і миру. Вони залишаються важливим інструментом забезпечення та захисту національних інтересів держав та регулювання міжнародних відносин. Людство сьогодні живе в умовах відносно стабільної рівноваги між силами аргументації (політико-дипломатичної, економічної і т.д.) і аргументами сили.

Природно, кожна держава має свою особливу структуру національних інтересів і, відповідно, свої власні пріоритети і основні шляхи їх досягнення. Для забезпечення загальної стабільності, безпеки і миру важливо в принципі, щоб взаємозв'язок між державами визначалася не формулою «панування-підпорядкування,» яка передбачає задоволення власних інтересів за рахунок інших, а на основі співіснування, співпраці, взаємної вигоди, партнерства рівних прав і добросусідства.

Сили забезпечення національної безпеки включають в себе ЗСУ, інші війська, військові формування і відомства, в яких відповідно до законодавства України передбачена військова служба, а також структурні підрозділи органів виконавчої влади, на які покладаються функції щодо забезпечення національної безпеки. Повноваження сил забезпечення національної безпеки визначаються відповідними законодавчими актами.

Система захисту національних інтересів України в галузі економіки базується на встановленні та нормативно-правовому закріпленні обов'язкових процедур з формування цільових установок, програмних заходів і дій, що забезпечують виявлення, локалізацію та протидію загрозам економічній безпеці

країни;

– правові заходи-вимоги дотримання норм міжнародного права, договорів і угод, положень; шляхом підписання двосторонніх і багатосторонніх договорів та угод з врегулювання правових взаємовідносин; використання юридичних засобів і міжнародних правових інститутів (Міжнародний суд ООН, Європейський суд та ін.);

- військові заходи – вираження проведення регулярних збройних сил на штати воєнного часу, резервів на воєнний стан; створення нових з'єднань та частин; перебазування та розосередження сил та засобів військової авіації і флоту; демонстрація оперативного розгортання з'єднань і частин уздовж державного кордону;

- інформаційно-психологічні заходи-пропаганда необхідності дотримання міжнародних договорів та угод; психологічно-інформаційний вплив на державу з метою утримання їх від надання безпосередньої допомоги країнам, які готують конфлікт (приймають участь в конфлікті); інформування населення і війська про причини і справжні цілі конфлікту; Інформаційно-психологічні операції щодо запобігання розпалювання національної ворожнечі та ін. деструктивних настроїв і дій;

- військово-технічні заходи-створення і підтримка цілісної системи озброєння України, що представляє собою взаємопов'язану сукупність озброєння ЗСУ, інших військ, військових формувань і органів, що забезпечує вирішення завдань оборони і безпеки країни на необхідному рівні.

При вирішенні певних і непередбачених завдань забезпечення національної безпеки в режимі звичайних, оптимальних і екстремальних умов велику роль відіграють різного роду ресурси, що представляють собою сукупність відомих на даний момент засобів і джерел їх отримання.

Види забезпечення національної безпеки передбачають вирішення проблем національної безпеки в різних сферах суспільного життя і людської діяльності: політичної, економічної, соціальної, військової, інформаційної, екологічної та ін всі види забезпечення національної безпеки тісно

взаємопов'язані і взаємно доповнюють один одного (наприклад, військова безпека не може бути забезпечена при слабкій і неефективній економіці). Кожен з видів забезпечення національної безпеки залежно від характеру джерел загроз має зовнішній і внутрішній аспекти. Залежно від об'єкта, життєво важливі інтереси якого захищаються від внутрішніх і зовнішніх загроз, виділяються такі види забезпечення національної безпеки, як безпека особистості, суспільства, держави та інших об'єктів.

Як показало дослідження, проведене на основі звіту «Глобальний індекс кібербезпеки», опубліковане Міжнародним союзом електрозв'язку (ITU) в 2018 році, низький рівень стандартизації в області кібербезпеки для організацій є однією з найголовніших проблем інформаційної безпеки України [31].

Стандартизація в галузі інформаційних технологій спрямована на підвищення ступеня відповідності функціональному призначенню типів інформаційних технологій, складових їх компоненти і процеси, долаючи технічні бар'єри в міжнародному інформаційному обміні.

Стандарти забезпечують головну можливість розробникам таких інформаційних технологій, що використовують дані, комунікаційні засоби інших розробників, програмні, інтеграцію різних компонентів інформаційних технологій, здійснювати експорт / імпорт даних.

Наприклад, для регламентації взаємодії між різними програмами призначені стандарти міжпрограмного інтерфейсу (один з них – стандарт технології OLE (Object Linking and Embedding – вбудовування та зв'язування таких об'єктів). Саме без таких стандартів програмні продукти були б абсолютно «закритими» один для одного.

Вимоги користувачів по стандартизації в сфері інформаційних технологій реалізуються в стандартах на користувальницький інтерфейс, наприклад, в стандарті GUI (Graphical User Interface).

Стандарти займають все більше важливе місце в напрямку розвитку індустрії інформаційних технологій. Вже понад 1000 стандартів або вже повністю прийняті організаціями зі стандартизації, або перебувають в процесі

розробки. Процес стандартизації інформаційних технологій ще не закінчений.

Так що ж таке стандарт? Стандарт – це документ, що встановлює вимоги, специфікації, керівні принципи або характеристики, відповідно до яких можуть використовуватися матеріали, Продукти, процеси і послуги, які підходять для цих цілей. ISO опублікувала понад 19000 міжнародних стандартів, які можуть бути отримані від ISO або її членів.

Стандарт також має містити конкретні вимоги до символіки, термінології, маркування, упаковки або етикетування, правила і методи досліджень (випробувань) і вимірювань, правила відбору зразків.

Стандарти інформаційної безпеки – це загально обов'язкові або рекомендовані до впровадження документи, в яких визначено підходи до оцінки рівня ІБ та встановлено вимоги до безпечних інформаційних систем [6].

Стандарти в області інформаційної безпеки виконують наступні найважливіші функції:

- вироблення понятійного апарату та термінології в галузі інформаційної безпеки;

- підвищення технічної та інформаційної сумісності продуктів, що забезпечують ІБ;

- узгоджена оцінка продуктів, що забезпечують інформаційну безпеку;

- формування шкали вимірювань рівня інформаційної безпеки;

- функція нормотворчості-надання деяким стандартам юридичної сили і встановлення вимоги їх обов'язкового виконання;

- накопичення відомостей про кращі практики забезпечення інформаційної безпеки та їх надання різним групам зацікавленої аудиторії-адміністраторам та користувачам інформаційних систем, виробникам засобів ІБ, ІТ-директорам, експертам [26].

Завдяки стандартам інформаційної безпеки:

1. Виробники та експерти: обґрунтовано визначають Набори вимог до інформаційних продуктів і декларують їх можливості; підтверджують цінність продуктів шляхом сертифікації на відповідність стандартам ІБ; отримують

цінну технічну та іншу інформацію.

2. Споживач: обґрунтовано вибирають інформаційні продукти; більш чітко формулюють вимоги до них; мають можливість побудувати гарантовано якісну систему ІБ.

Головними областями стандартизації інформаційної безпеки є: моделі інформаційної безпеки; безпека міжмережевих взаємодій; аудит інформаційної безпеки; криптографія; методи і механізми забезпечення інформаційної безпеки; управління інформаційною безпекою.

Об'єктом стандартизації може бути абсолютно будь-який продукт чи послуга ІБ: метод оцінки, функціональні можливості засобів захисту та параметри настройки, властивості сумісності, процес розробки і виробництва, системи менеджменту і т. д.

Стандартизація, залежно від складу її учасників, може бути національною, регіональною або міжнародною, при цьому Міжнародна стандартизація (нарівно з офіційними органами стандартизації, такими як ISO) включає в себі стандартизацію певних консорціумів (таких, як IEEE або SAE), а Національна стандартизація буває державною або галузевою.

Стандартизація в області інформаційної безпеки (ІБ) корисна і професіоналам, і споживачам продуктів та послуг ІБ, так як дозволяє встановити оптимальний рівень упорядкування та уніфікації, досягти взаємозамінність продуктів ІБ, та повторюваність і вимірюваність результатів, що отримуються в різних країнах та організаціях. Для професіоналів-спеціалістів –це суттєва економія часу на пошук продуктивних та рекомендованих рішень, а для споживача – це перш за все, гарантія отримання результату очікуваної якості.

Саме тому стандартизація в галузі інформаційної безпеки необхідна і вимагає якнайшвидших перетворень, що дозволить удосконалити механізм забезпечення інформаційної безпеки держави.

# ВИСНОВКИ

Інформатизація суспільства створює безліч проблем у сфері інформаційної безпеки, головними з яких є: проблеми інформаційних воєн та інформаційного тероризму. Вони носять не тільки глобальний характер, але і надають особливу гостроту для нашої країни, що обумовлено її геополітичними та економічними інтересами.

Інформаційна безпека держави – захист конституційного ладу, суверенітету, територіальної цілісності з використанням інформаційних засобів. Життєво важливі інтереси держави в інформаційній сфері:

- формування таких інститутів громадського контролю за діяльністю органів державної влади;
- створення умов для реалізації інтересів особистості та суспільства в інформаційній сфері;
- безумовне забезпечення законності та правопорядку;
- створення умов для розвитку власної інформаційної інфраструктури;
- формування системи підготовки та реалізації рішень органів державної влади, що забезпечують національні інтереси країни;
- захист державної інформаційної системи та інформаційних ресурсів у тому числі захист державної таємниці;
- захист єдиного інформаційного простору країни;
- розвиток рівноправного і взаємного міжнародного співробітництва.

Національна безпека України залежить в ключовому значенні від стану забезпечення інформаційної безпеки, та в ході сучасного технічного прогресу ця залежність від інформаційної безпеки буде багаторазово зростати.

Під інформаційною безпекою України ми розуміємо стан захищеності саме її національних інтересів в інформаційній сфері, що проявлються сукупністю збалансованих інтересів індивіда, зокрема, суспільства і держави в цілому. Саме на основі національних інтересів України саме в інформаційній сфері формуються стратегічні та поточні завдання внутрішньої і зовнішньої

політики держави щодо забезпечення інформаційної безпеки.

Загрози інформаційній безпеці держави: розмивання єдиного правового простору країни через прийняття певними регіонами країни, що не відповідали Конституції України правових актів; руйнування єдиного інформаційного простору України; витіснення українських інформаційних агентств і засобів масової інформації з внутрішнього інформаційного ринку; монополізація інформаційного ринку; блокування роботи державних засобів масової інформації щодо інформування української, зарубіжної аудиторії; ослаблення ролі української мови як державної мови України; несанкціоноване цілеспрямоване втручання і проникнення в діяльність і розвиток інформаційних систем; низька ефективність інформаційного забезпечення державної політики (дефіцит кадрів, відставання інформаційних систем від міжнародних стандартів).

Загрози інформаційної безпеки України можна розділити за загальною спрямованістю, а саме загрози конституційним правам і свободам громадян, духовному життю суспільства, інформаційній структурі, інформаційним ресурсам і за способами впливу – інформаційні, програмно-математичні, фізичні та організаційні.

На сучасному етапі розвитку суспільства проблема інформаційної безпеки залишається бути актуальною і потребує її вирішення. Інформаційна безпека є ключовим компонентом, зокрема економічної безпеки та національної безпеки країни в цілому. Від неї значною мірою залежить рівень і інших видів безпеки, а саме: оборонної, соціальної та політичної.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бакуменко В. Д. Формування державно-управлінських рішень: Проблеми теорії, методології, практики : монографія / В. Д. Бакуменко. К. : Вид-во УАДУ, 2000. 328 с.

2. Бодрук О. Національні інтереси / О. Бодрук // Політика і час. 2001. № 12. С. 52-62.

3. Бодрук О. С. Структури воєнної безпеки: національний та міжнародний аспекти : монографія / О. С. Бодрук. К. : НІПМБ, 2001. 300 с.

4. Валевський О. Л. Державна політика в Україні: методологія аналізу, стратегія, механізми впровадження : монографія / О. Л. Валевський. К. : НІСД, 2001. 240 с.

5. Воєнна безпека України на межі тисячоліть : монографія / Г. М. Перепелиця, С. О. Дмитрова, В. С. Корсидович та ін. К. : Стилос, 2002. 384 с.

6. Глобалізація і безпека розвитку : монографія / О. Г. Білорус, Д. Г. Лук'яненко та ін. ; керів. авт. кол. і наук. ред. О. Г. Білорус. К. : КНЕУ, 2001. 733 с.

7. Демченко П. Кібернетична безпека як новітній напрям інформаційної складової національної безпеки України: конституційно-правовий аспект. URL: http://publications.lnu.edu.ua/bulletins/index.php/law/article/view/9560.

8. Доктринальні положення інформаційної безпеки України в умовах сучасності [Електронний ресурс] // LEXINFORM.COM.UA. – 2019. – URL: https://lexinform.com.ua/dumka-eksperta/doktrynalni-polozhennya-informatsijnoyi-bezpeky-ukrayiny-v-umovah-suchasnosti/.

9. Закон України про основи національної безпеки України // Уряд. кур'єр. 2003. 30 лип.

10. Закон України про Раду національної безпеки і оборони України // Голос України. 1998. 3 квіт.

11. Засади національної безпеки України : підручник / В. П. Горбулін, А. Б. Качинський. К. : Інтертехнологія, 2009. 272 с.

12. Інформаційна війна і національна безпека : монографія / П.П. Ткачук, Р.В. Гула, О.І. Сивак, О.М. Щурко, В.В. Шемчук. Львів: НАСВ, 2015. 265 с.

13. Камінська Н.В. Міжнародна інформаційна безпека в умовах глобалізації та інтеграції. Міжнародне право: виклики сьогодення : матер. Міжнар. науково-практ. конф. (Київ, 20 грудня 2016 р.) Київ, 2016. С. 22–27.

14. Косогов О.М. Інформаційна безпека у сфері оборони як складова воєнної безпеки України. Системи обробки інформації. 2016. Вип. 8 (145). С. 115–117.

15. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії) : автореф. дис. ... канд. політ. наук. Київ, 1997.18 с.

16. Наливайко Л. Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект. Вісник Запорізького державного університету. 2003. № 1. С. 60–65.

17. Національна безпека України: теорія і практика : навч. посіб. / Г. П. Ситник, В. М. Олуйко, М. П. Вавринчук ; за заг. ред. Г. П. Ситника. Хмельницький ; К. : Кондор, 2007. 616 с.

18. Постанова Кабінету Міністрів України від 14 січня 2015 р. № 2 «Питання діяльності Міністерства інформаційної політики України»

19. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 № 75/98-ВР. URL: http://zakon4.rada.gov.ua/l.

20. Про оборону України : Закон України. Відомості Верховної Ради України. 1992. № 9. Ст. 106 (у редакції від 03.07.2019). URL: http://zakon4.rada.gov.ua/laws/show/1932-12.

21. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. № 964 - IV.

22. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 № 537-V. URL: http://zakon4.rada.gov.ua/l.

23. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про скасування деяких рішень Ради національної безпеки і оборони України» та визнання такими, що втратили чинність, деяких указів Президента України http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&

24. Соловйов С.Г. Теоретичні засади інформаційної оборони. Державне будівництво. 2015. № 1. URL: http://www.kbuapa.kharkov.ua/e-book/db/2015-1/doc/1/06.pdf.

25. Сушко О., Зелінська О., Хорольський Р., Мовчан В., Солоненко І., Гуменюк В., Трюхан В. Угода про асоціацію. Україна – ЄС: дороговказ реформ. URL : http:// www.kas.de/ukraine/ukr/publications/32048.

26. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів [Електронний ресурс] / Н. Тарасенко //Резонанс. 2017. № 18. С. 3–14. – Режим доступу: http://nbuviap.gov.ua/images/rezonans/2017/rez18.pdf.

27. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 422 с.

28. Указ Президента України від 26 травня 2015 року № 287/2015 «Про Стратегію національної безпеки України». URL: https://www.president.gov.ua/documents/2872015-19070.

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

30. Харченко Л.С., Ліпкан В.А., Логінов О.В. Інформаційна безпека України: Глосарій / за заг. ред. Р.А. Калюжного. Київ: Текст, 2004. 180 с.

31. Це рейтинг країн за рівнем кібербезпеки. Україна – на 25-му місці [Електронний ресурс] // The Village Україна. – 2020. – URL: https://www.the-village.com.ua/village/business/news/305021-tse-reyting-krayin-za-rivnem-kiberbezpeki-ukrayina-na-25-mu-mistsi.

32. Шемчук В.В. Теоретико-правові засади дослідження інформаційної безпеки. Європейські перспективи. 2019. № 2. С. 5–11.

33. Юридична енциклопедія : у 6 т. / редкол.: Ю.С. Шемшученко (відп. ред.) та ін. Київ: Укр. енциклопедія, 1998-1999. Т. 2 : Д-Й. 744 с.