

Київський національний торговельно-економічний університет  
Кафедра публічного управління та адміністрування

**ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА**  
на тему:  
**МЕХАНІЗМ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ**  
**ВІД ЗОВНІШНІХ ВПЛИВІВ**

Студента 2-го курсу, 4-м групи,  
спеціальності 281 «Публічне  
управління та адміністрування»  
спеціалізації «Публічне  
управління та адміністрування»

\_\_\_\_\_  
(підпис студента)

Небога  
Ігор  
Владиславович

Науковий керівник  
к.е.н.,  
доцент

\_\_\_\_\_  
(підпис керівника)

Сонько  
Юлія  
Анатоліївна

Гарант освітньої програми  
д-р. екон. наук,  
доцент

\_\_\_\_\_  
(підпис гаранта)

Ладонько  
Людмила  
Степанівна

Київ 2020

**Київський національний торговельно-економічний університет**

Факультет економіки, менеджменту та психології

Кафедра публічного управління та адміністрування

Освітній ступінь: магістр

Спеціальність: публічне управління та адміністрування

Спеціалізація: публічне управління та адміністрування

**Затверджую**

Зав.кафедри \_\_\_\_\_

«28» лютого 2020р.

**Завдання  
на випускню кваліфікаційну роботу (проект)  
студентові**

**Небозі Ігорю Владиславовичу**

(прізвище, ім'я, по батькові)

**Тема випускної кваліфікаційної роботи(проекту): «МЕХАНІЗМ ЗАХИСТУ  
ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ВІД ЗОВНІШНІХ  
ВПЛИВІВ»**

Затверджена наказом ректора від «27»лютого 2020 р.№756

1. Строк здачі студентом закінченого роботи(проекту): 02.11.2020

2. Цільова установка та вихідні дані до роботи(проекту)

*Мета роботи(проекту):* обґрунтування організаційно-правових механізмів захисту інформаційного простору України від зовнішніх впливів.

*Об'єкт дослідження:* процес формування системи захисту інформаційного простору України.

*Предмет дослідження:* теоретико-методичні та прикладні основи механізмів захисту інформаційного простору України.

3. Зміст випускної кваліфікаційної роботи (проекту)  
(перелік питань за кожним розділом):

ВСТУП

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ СИСТЕМИ  
ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

РОЗДІЛ 2. АНАЛІЗ МЕХАНІЗМІВ ДЕРЖАВНОЇ ПОЛІТИКИ У  
СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

- 2.1. Аналіз організаційно-правових механізмів державної  
політики у сфері захисту інформаційного простору
- 2.2. Нормативно-правове регулювання захисту інформаційного  
простору в Україні

РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ  
ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ  
ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В УКРАЇНІ ВІД  
ЗОВНІШНІХ ВПЛИВІВ

- 3.1. Обґрунтування необхідності створення ефективної системи  
захисту інформаційного простору, з метою забезпечення  
інформаційного суверенітету України
- 3.2. Шляхи вдосконалення механізму захисту інформаційного  
простору України від зовнішніх впливів

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ  
ДОДАТКИ

4. Календарний план виконання роботи(проекту)

| №<br>пор. | Назва етапів випускної кваліфікаційної<br>роботи (проекту)                                  | Строк виконання<br>етапів роботи |            |
|-----------|---------------------------------------------------------------------------------------------|----------------------------------|------------|
|           |                                                                                             | за планом                        | фактично   |
| 1         | 2                                                                                           | 3                                | 4          |
| 1         | Визначення напрямку дослідження та<br>затвердження теми випускної<br>кваліфікаційної роботи | До 01.11.2019                    | 01.11.2019 |
| 2         | Складання плану та підготовка                                                               | До 28.02.2020                    | 28.02.2020 |



|    |                                                                                                                    |                   |                   |
|----|--------------------------------------------------------------------------------------------------------------------|-------------------|-------------------|
|    | індивідуального завдання для виконання<br>випускної кваліфікаційної роботи                                         |                   |                   |
| 3  | Представлення на рецензування науковому<br>керівнику рукопису першого розділу<br>випускної кваліфікаційної роботи  | До 19.06.2020     | 19.06.2020        |
| 4  | Представлення на рецензування науковому<br>керівнику рукопису другого розділу<br>випускної кваліфікаційної роботи  | До 01.09.2020     | 01.09.2020        |
| 5  | Представлення на рецензування науковому<br>керівнику рукопису третього розділу<br>випускної кваліфікаційної роботи | До 01.10.2020     | 01.10.2020        |
| 6  | Представлення закінченої випускної<br>кваліфікаційної роботи на кафедрі                                            | До 02.11.2020     | 02.11.2020        |
| 7  | Підготовка письмового відгуку на<br>випускні кваліфікаційні роботи                                                 | До 06.11.2020     | 06.11.2020        |
| 8  | Зовнішнє рецензування ВКР                                                                                          | До 16.11.2020     | 16.11.2020        |
| 10 | Проведення попереднього захисту<br>випускних кваліфікаційних робіт                                                 | 23-27.<br>11.2020 | 23-27.<br>11.2020 |
| 11 | Вирішення питання про допуск випускної<br>кваліфікаційної роботи до захисту                                        | До 01.12.2020     | До 01.12.2020     |
| 12 | Направлення випускної кваліфікаційної<br>роботи із зовнішньою рецензією до ЕК для<br>захисту                       | За графіком       | За графіком       |

5. Дата видачі завдання «28» лютого 2020 р.

6. Науковий керівник випускної кваліфікаційної роботи (проекту)

Сонько Ю.А.

(прізвище, ініціали, підпис)

7. Керівник проектної групи (гарант освітньої програми) Ладонько Л.С.

(прізвище, ініціали, підпис)

8. Завдання прийняв до виконання студент: Небога І.В.

(прізвище, ініціали, підпис)

9. Відгук наукового керівника випускної кваліфікаційної  
роботи (проекту):

Тема ВКР є актуальною в сучасних умовах. У першому розділі зроблено спробу розкрити сутнісні характеристики інформаційного простору та інформаційної безпеки та визначити нормативно-правове забезпечення в інформаційній сфері.

У другому розділі студентом проведено оцінювання стану організаційно-правових механізмів державної політики в інформаційній сфері та викладено пропозиції щодо удосконалення механізмів, що забезпечують ефективне функціонування інформаційних ресурсів.

У третьому розділі визначено основні загрози інформаційній безпеці України та розроблено практичні рекомендації щодо вдосконалення організаційно-правових механізмів в інформаційній сфері.

Одержані результати можуть бути використані при удосконаленні роботи Міністерства культури та інформаційної політики.

Загалом робота виконана на відповідному рівні, відповідає встановленим вимогам та може бути допущена до захисту.

Науковий керівник випускної кваліфікаційної роботи  
(проекту) Сонько Юлія Анатоліївна

*(підпис, дата)*

#### 10. Відмітка про попередній захист

Ладонько Людмила Степанівна

*(ПІБ, підпис, дата)*

#### 11. Висновок про випускну кваліфікаційну роботу (проект):

Випускна кваліфікаційна робота (проект) студента Небоги І.В. може бути допущена до захисту екзаменаційній комісії.

Керівник проектної групи (гарант освітньої програми): Ладонько  
Людмила Степанівна

*(прізвище, ініціали, підпис)*

Завідувач кафедри: Новікова Наталія Леонідівна

*(підпис, прізвище, ініціали)*

«03» грудня 2020 р.

## ЗМІСТ

|                                                                                                                                                                     |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| <b>ВСТУП</b> .....                                                                                                                                                  | 2  |
| <b>РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ</b> .....                                                                 | 4  |
| <b>РОЗДІЛ 2. АНАЛІЗ МЕХАНІЗМІВ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ</b> .....                                                                           | 13 |
| <b>2.1. Аналіз організаційно-правових механізмів державної політики у сфері захисту інформаційного простору</b> .....                                               | 13 |
| <b>2.2. Нормативно-правове регулювання захисту інформаційного простору в Україні</b> .....                                                                          | 21 |
| <b>РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В УКРАЇНІ ВІД ЗОВНІШНІХ ВПЛИВІВ</b> .....   | 28 |
| <b>3.1. Обґрунтування необхідності створення ефективної системи захисту інформаційного простору, з метою забезпечення інформаційного суверенітету України</b> ..... | 28 |
| <b>3.2. Шляхи вдосконалення механізму захисту інформаційного простору України від зовнішніх впливів</b> .....                                                       | 34 |
| <b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ</b> .....                                                                                                                             | 44 |
| <b>ДОДАТКИ</b> .....                                                                                                                                                | 51 |



## ВСТУП

**Актуальність теми:** В умовах розвитку інформаційного суспільства та широкосмугового доступу до мережі Інтернет зростає значення інформаційного захисту та інформаційної безпеки держави. Необхідність гарантування інформаційної безпеки як змістовної складової національної безпеки зумовлюється існуванням загроз для інформаційної сфери країни, що можуть спричинити негативний вплив на свідомість населення України.

У сучасних умовах конфлікту на Сході України дослідження питань, пов'язаних з безпекою інформаційного простору держави від негативних проявів, спрямованих на завдання шкоди національним інтересам в інформаційній сфері та наукове обґрунтування впровадження системної і збалансованої державної інформаційної політики, здатної забезпечити захист суспільства, держави і громадян від інформаційної та інформаційно-психологічної експансії суб'єктів геополітичної конкуренції та інших загроз, набуває особливої важливості.

**Метою роботи** є обґрунтування організаційно-правових механізмів захисту інформаційного простору України від зовнішніх впливів.

**Об'єктом дослідження** є процес формування системи захисту інформаційного простору України.

**Предметом дослідження** є теоретико-методичні та прикладні основи механізмів захисту інформаційного простору України.

Різні аспекти проблеми захисту інформаційного простору України від зовнішніх впливів висвітлені у працях таких вітчизняних вчених, як: К. Лобузін[3], Б. Кормич[6], Ю. Іванченко[20] В.Петрик[25], О.Юдін[35], Т.Ткачук[44], О.Гіда[49]. Вивчення праць вказаних науковців дозволяє ґрунтовно підійти до дослідження сутності поставленого наукового завдання.

**Обрана мета обумовила виконання наступних завдань:**

- визначити сутність понять «інформаційний простір» та «інформаційна безпека»;
- визначити основні проблеми захисту інформаційного простору України;
- проаналізувати нормативно -правове забезпечення в інформаційній сфері;

- дослідити стан організаційно-правових механізмів державної політики в інформаційній сфері;
- визначити основні напрями державної інформаційної політики;
- проаналізувати механізми, що забезпечують ефективне функціонування інформаційних ресурсів;
- визначити основні загрози інформаційній безпеці України;
- розробити рекомендації щодо шляхів вдосконалення організаційно-правового забезпечення у сфері захисту інформаційного простору України.

З метою реалізації поставлених завдань використано загальнонаукові та спеціальні методи дослідження: наукової абстракції – для розкриття понять «інформаційний простір» та «інформаційна безпека» та формування об’єкта дослідження; аналізу та синтезу – для виявлення необхідності створення ефективної системи захисту інформаційного простору; логічний метод – для формування шляхів вдосконалення організаційно-правових механізмів захисту інформаційного простору України від зовнішніх впливів.

Інформаційною базою дослідження стали: Конституція України, Закони України, оперативна інформація міністерств та відомств, праці вітчизняних і зарубіжних науковців з проблеми дослідження, а також інформаційні ресурси мережі Інтернет.

Випускна кваліфікаційна робота складається зі вступу, 3 розділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 52 сторінки, з них основного тексту 42 сторінки, в т.ч. 1 таблиця та 9 рисунків.

Список використаних джерел містить 55 найменувань, викладених на 7 сторінках, робота містить 2 додатки на 2 сторінках.

Результати дослідження опубліковано: Небога І. Теоретичні основи формування системи захисту інформаційного простору України / І. Небога // Публічне управління та адміністрування в умовах суспільних трансформацій : зб. наук. ст. студ. відп. ред. Н.Л. Новікова. – К.: Київ. нац. торг.-екон. ун-т, 2020. – 251 с., С. 168-174.



## **РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ**

Зміцнення та захист національного інформаційного простору України є складовою частиною забезпечення її національної безпеки. У сучасних реаліях військовий конфлікт на Сході України доводить те, що завоювання частини територій призвело до втрати контролю над інформаційним полем України і загрожує масовим розповсюдження інформаційного на культурного продукту супротивника.

Враховуючи, усі ці фактори дослідження питань, які безпосередньо пов'язані з безпекою інформаційного простору країни від негативних зовнішніх впливів, спрямованих на завдання шкоди національним інтересам в інформаційній сфері та наукове обґрунтування необхідності впровадження збалансованої державної політики в цій сфері, здатної забезпечити захист суспільства, держави і громадян від інформаційної та інформаційно-психологічної експансії суб'єктів геополітичної конкуренції та інших загроз, набуває особливої важливості. Підтримання важливих зовнішньо-політичних рішень та пошук нових підходів до управління в сфері інформації є першочерговими кроками для побудови сприятливого іміджу України[1].

Термін «інформаційний простір» є багатогранним поняттям і немає єдиного значення. У філософсько-методологічному вимірі під інформаційним простором розуміється поширення інформації у соціумі.

Д. Белл розглядає інформаційний простір як сукупність знань, що мають цінність у вигляді економічного ресурсу, який сприяє розвитку тих чи інших секторів громадського життя. Специфіка інформації, з такої точки зору, полягає в здатності слугувати товаром, брати участь в економічних маніпуляціях і бути запорукою економічної стабільності.

Фурашев В.М. вважає, що інформаційний простір – це форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот. Об'єктами інформаційного

простору є суб'єкти природного середовища, природні та штучні інформаційні відносини між ними та їх створення і використання. Матеріальні та нематеріальні об'єкти і процеси, спрямовані на задоволення інформаційних потреб та для забезпечення життєдіяльності однієї істоти або угруповання живих істот. Відповідно, суб'єкти інформаційного простору це живі істоти та групи осіб, які спроможні сприймати, запам'ятовувати та обробляти інформацію, а також обмінюватися нею[2].

Інформаційний простір має властивості такі характерні ознаки як:

- протяжність;
- єдність неперервності та дескретності;
- матеріальність та нематеріальність;
- дійсність і абстрактний прояв;
- реальність загальнодіючого впливу.

Лобузіна К.В. визначає інформаційний простір не лише як технологічну базу, комп'ютерно-телекомунікаційне обладнання, засоби доступу до даних та канали зв'язку, а як систему відносин між тими, хто виробляє, зберігає і розповсюджує інформацію та між споживачами інформації, тобто між усіма учасниками сучасної системи інформаційних комунікацій[3].

Є. А. Макаренко у дослідженні “Європейська інформаційна політика” під єдиним інформаційним простором країни пропонує розуміти сукупність інформаційних ресурсів та інформаційної інфраструктури, що на основі єдиних принципів і за загальними правилами дозволяє забезпечувати безпечну інформаційну взаємодію держави, організацій і громадян і їх рівний доступ до відкритих інформаційних ресурсів, а також максимальне задоволення їхніх інформаційних потреб на усій території держави за збереження балансу інтересів на входження у світовий інформаційний простір і забезпечення національного інформаційного суверенітету[4].

Згідно Концепції інформаційної безпеки України національний інформаційний простір – це сукупність всіх національних та іноземних інформаційних потоків, до яких є доступ на території держави[5].

Захист інформаційного простору можна визначити як сукупність спеціальних заходів спрямованих на зміцнення інформаційного суверенітету та протидію інформаційній агресії та блокаді, які проявляються з боку індивідів, груп людей та інших країн.

Захист інформаційного простору тісно пов'язаний із поняттям інформаційної безпеки, яка може бути розглянута як захищеність різних галузей інформації.

На думку Б.Кормича, інформаційна безпека – це захищеність правил, встановлених законом, за якими здійснюються інформаційні процеси в державі, що в свою чергу забезпечують гарантовані Конституцією умови існування і розвитку людини, держави та суспільства загалом[6].

О.Л. Сорокін вважає, що інформаційна безпека – це такий стан захищеності інформаційної інфраструктури, включаючи також комп'ютери та інформаційно-телекомунікаційну інфраструктуру та інформацію, що в них знаходиться[7].

На думку І. Громико, Т. Саханчук, інформаційна безпека – це стан захищеності державних інтересів, який досягається шляхом моніторингу, виявлення і знищення, як внутрішніх, так і зовнішніх інформаційних загроз, та забезпечення міжнародного співробітництва у цій сфері[8].

Інформаційна безпека держави є важливим елементом усіх сфер національної безпеки країни. В той же час інформаційна безпека – це окрема та незамінна галузь забезпечення національної безпеки, що визначає стан захищеності національних інтересів від різноманітних загроз і являє собою сукупність інформаційно-психологічної та інформаційно-технологічної безпеки держави[9].

Потреба забезпечення національної безпеки країни в цілому, існування та поширення загроз в інформаційній сфері, які можуть завдавати значної шкоди національним інтересам держави, той факт, що допомогою інформації можна впливати на поведінку людей та змінювати їх свідомість – все це зумовлює необхідність гарантування інформаційної безпеки в Україні. Завданням



інформаційної безпеки є розробка системи захисту інформаційного простору країни, її інформаційних ресурсів та інфраструктури[10].

Центральним органом, який здійснює координацію та контроль забезпечення інформаційної безпеки як складової національної безпеки і оборони в межах компетенції та покладених на нього функцій є Рада національної безпеки і оборони України, яка формулює стратегічні національні інтереси України, підходи та напрями забезпечення інформаційної безпеки.

Для визначення актуальних і коректних напрямів діяльності, спрямованої на захист інформаційного простору від зовнішніх впливів, необхідно врахувати основні проблеми захисту інформаційного простору України (Рис.1.1) :



**Рис.1.1 Основні проблеми захисту інформаційного простору України**

*Джерело:* побудовано автором за матеріалами[5]

Для створення ефективної системи захисту національного інформаційного простору необхідним є наявність якісного нормативно-правового забезпечення у цій сфері. Уже існуючі нормативно-правові акти сформували певне законодавче поле для діяльності органів державної влади та суспільства загалом, а також стали фундаментом для розбудови нормативно-правового забезпечення нового типу, що

відповідає сучасним реаліям ідеологічного протистояння, що загрожує недоторканості інформаційного простору України.

Нормативно-правове регулювання системи забезпечення інформаційної безпеки України представлено: Конституцією України та законами України «Про інформацію», «Про основи національної безпеки України», «Про Концепцію Національної програми інформатизації», «Про телебачення та радіомовлення», «Про інформаційні агентства», «Про державну таємницю», «Про зв'язок», «Про друковані засоби масової інформації (пресу) в Україні», «Про державну підтримку засобів масової інформації та соціальний захист журналістів» та іншими нормативно -правовими актами.

У ст. 17. Конституції України зазначено: “Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу”

Згідно Закону України «Про інформацію», який є одним із основних нормативно-правових актів у цій сфері, захист інформації – це сукупність правових, технічних, організаційних, адміністративних заходів, що забезпечують збереження інформації, її цілісність та врегульований порядок доступу до неї. Право громадян на інформацію охороняється чинним законодавством, держава забезпечує рівні права і можливості доступу до інформації всім суб'єктам інформаційних відносин, права особи у виборі форм і джерел одержання інформації не можуть бути обмежені, за винятком випадків, які передбачені законом. Цей Закон забороняє знищення та конфіскацію друкованих видань, інформаційних банків, експонатів, документів з музейних, бібліотечних, архівних фондів, окрім випадків встановлених законом або на підставі рішення суду[11].

Відповідно до Закону України «Про основи національної безпеки України» державна політика у сферах національної безпеки і оборони спрямована на забезпечення воєнної, внутрішньодержавної, зовнішньополітичної, екологічної, економічної та інформаційної безпеки. Державним органом, призначеним для



забезпечення розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах критичної інформаційної інфраструктури, кіберзахисту, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, технічного та криптографічного захисту інформації, телекомунікацій, використання радіочастотного ресурсу України, поштового зв'язку спеціального призначення є Державна служба спеціального зв'язку та захисту інформації України[12].

У Законі України “Про основи національної безпеки України” визначено основні напрямки державної політики з питань національної безпеки в інформаційній сфері. До них належать:

- забезпечення інформаційного суверенітету України;
- покращення заходів щодо державного регулювання розвитку інформаційної сфери, за допомогою формування економічних і нормативно-правових передумов, які сприятимуть зміцненню інформаційних ресурсів та інформаційної, запровадження інноваційних технологій, а також поширення достовірної та позитивної інформації про Україну, як всередині країни, так і за її межами.
- постійне залучення ЗМІ до процесів боротьби з корупцією, випадками, коли публічні службовці зловживають своїм становищем та ситуаціями, які становлять загрозу інформаційній безпеці України;
- гарантування громадянам України конституційного права на доступ до інформації, на свободу слова, недопущення несанкціонованого втручання органів державної влади та органів місцевого самоврядування у професійну діяльність ЗМІ, дискримінації в інформаційній сфері і переслідування журналістів за їхні політичні позиції;
- реалізація комплексу заходів щодо захисту інформаційного простору та протидії монополізації інформаційної сфери України.



Згідно Концепції інформаційної безпеки України державна інформаційна політика зосереджена на задоволенні потреб і захисту інтересів громадянина, суспільства і держави в інформаційній сфері щодо[5]:

- створення, використання, поширення та розвитку національного медіа-контенту та інформації;
- роботи та захисту та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, які формують інфраструктуру внутрішнього інформаційного простору країни.

Питанням захисту національного інформаційного простору держава стала приділяти значно більше уваги після Революції Гідності. Першим кроком до створення дієвої загальнонаціональної системи захисту інформації стало Рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28.04.2014 року.

Згідно даного рішення КМУ необхідно було за один місяць розробити і запропонувати на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу. Служба безпеки України, а також Державна служба спеціального зв'язку та захисту інформації України зобов'язувалася за два місяці розробити та подати на затвердження Кабінету Міністрів України заходи, спрямовані на посилення захисту державних інформаційних ресурсів від протиправного втручання та ужити додаткових заходів щодо захисту інформації з обмеженим доступом[13].

Наступним кроком стало створення Міністерства інформаційної політики України 02.12.2014 р. МІП є «головним органом у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, зокрема, з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів» [14].

У своїй діяльності Міністерство інформаційної політики України базувалося виключно на принципах захисту свободи слова та думки, захисту прав громадян на вираження своєї позиції. При МІП створено Громадську раду, до якої входили представники громадських організацій та засобів масової інформації, науковці. Вона виконувала функції нагляду за діяльністю Міністерства та надавала поради щодо напрямів розвитку країни з впровадженням інформаційно-комунікаційних технологій.

Ключові завдання МІП було затверджено в Програмі дій Уряду, а також викладено у Коаліційній угоді між парламентськими фракціями Верховної Ради України. Такими завданнями є: створення стратегії інформаційної політики України та концепції інформаційної безпеки держави; координація органів влади в питаннях поширення інформації та комунікації; перешкоджання інформаційній агресії з боку країни-агресора. Основні завдання МІП [15]: узагальнення практик застосування законодавства з питань, що належать до його компетенції; здійснення нормативно-правового регулювання у сфері забезпечення інформаційного суверенітету України, в тому числі щодо розповсюдження суспільно важливої інформації в Україні та за її межами.

Постановою Кабінету Міністрів України від 2 вересня 2019 року Міністерство інформаційної політики реформувалося у Міністерство культури молоді та спорту. 23 березня 2020 року постановою Кабінету Міністрів України було затверджено рішення про перейменування Міністерства культури, молоді та спорту на Міністерство культури та інформаційної політики.

На нашу думку, Революція Гідності стала відправною точкою формування нової системи інформаційної безпеки України та стала сильним поштовхом для різких та якісних змін у сфері захисту інформаційного простору, якій до цього органи державної влади не надавали суттєвого значення.

Ми згодні з думкою Боднар І.Р. про те, що основні напрями інформаційної політики держави повинні базуватись на забезпеченні права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційну діяльність, недопущенні втручання в зміст та внутрішню організацію інформаційних процесів, зміцненні

та вдосконаленні вітчизняного національного інформаційного продукту та інформаційно-комунікаційних технологій, забезпеченні національно-культурної та інформаційної ідентифікації України у світовому інформаційному просторі, а також гарантуванні підтримки з боку держави та розвитку ресурсів науково-технічної продукції та інформаційних технологій[16].

Формування системи захисту інформаційного простору вимагає поєднання законодавчої та технічної складової. Окрім дієвих організаційно-правових механізмів, необхідним є також наявність матеріально-технічної бази та якісного програмного продукту, що забезпечить постійний моніторинг уже існуючих внутрішніх та зовнішніх загроз, попередження проявів потенційно-можливих загроз, а також швидкий та вільний доступ до достовірної інформації для громадян[17].

У сучасних умовах ведення військових дій на Сході України з кожним днем з'являються нові виклики і загрози для інформаційної безпеки, як складової національної безпеки України. Існуюча нормативно-правова база не враховує усі актуальні аспекти потенційно-можливих внутрішніх та зовнішніх інформаційних атак. Це пов'язано із швидким розвитком новітніх технологій, що дозволяють спростити процеси використання, доступу та передачі інформації, що загрожує безпеці інформаційних даних.

### **Висновки до розділу 1**

Отже, основним завданням суб'єктів забезпечення інформаційної безпеки України є проведення моніторингу загроз та реалізація сукупності заходів, спрямованих на захист інформаційного простору України. Роль держави у формуванні дієвої системи захисту інформаційного простору України є вирішальною, адже лише завдяки вдалому поєднанню інноваційних та організаційно-правових інструментів держава може перемогти у інформаційній боротьбі.



## **РОЗДІЛ 2. АНАЛІЗ МЕХАНІЗМІВ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

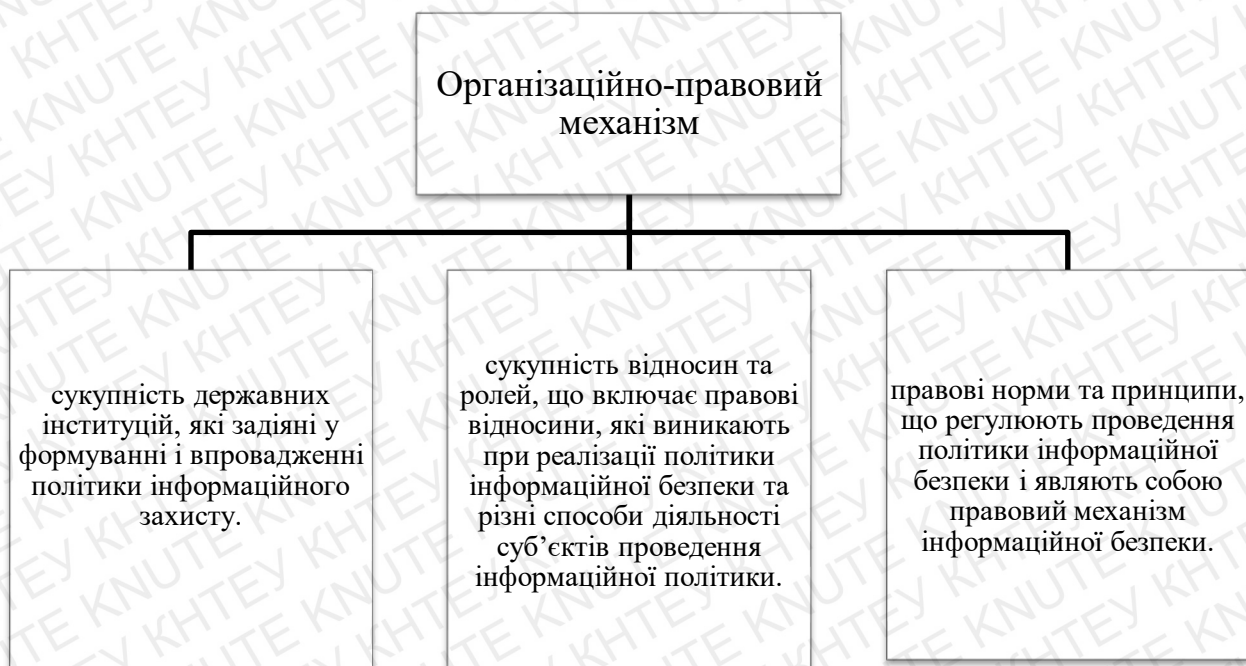
### **2.1. Аналіз організаційно-правових механізмів державної політики у сфері захисту інформаційного простору**

Сучасний стан суспільного розвитку та поява зовнішніх ризиків для інформаційного простору України зумовлюють необхідність посилення ролі держави у процесі забезпечення доступу громадян України до об'єктивної та оперативної інформації та гарантування захисту національного інформаційного простору від несприятливих інформаційних впливів.

Реалізація державної інформаційної політики повинна відбуватися на базі дієвих правових механізмів і організаційних заходів, результатом яких має стати відчутний позитивний ефект, а саме: недопущення незаконного поширення, використання та порушення цілісності інформації, гармонізація інтересів людини, суспільства і держави загалом в інформаційній діяльності [18].

Організаційно-правовий механізм інформаційної безпеки – це впорядкована сукупність державних інститутів, які задіяні у процесі розробки та імплементації політики інформаційної безпеки, відносини, внутрішні та зовнішні ролі якої регулюються системою певних принципів та норм права. Цей організаційно-правовий механізм складається з трьох основних елементів, які пов'язані між собою [19]. (Рис.2.1.)

Для забезпечення інформаційної безпеки держава визначає загрози такій безпеці та формує певні організаційно-правові інструменти, які застосовуються для протидії цим загрозам, враховуючи високий пріоритет прав і свобод людини і громадянина. Цей механізм сприяє формуванню відповідного вектору розвитку відносин у сфері інформації.



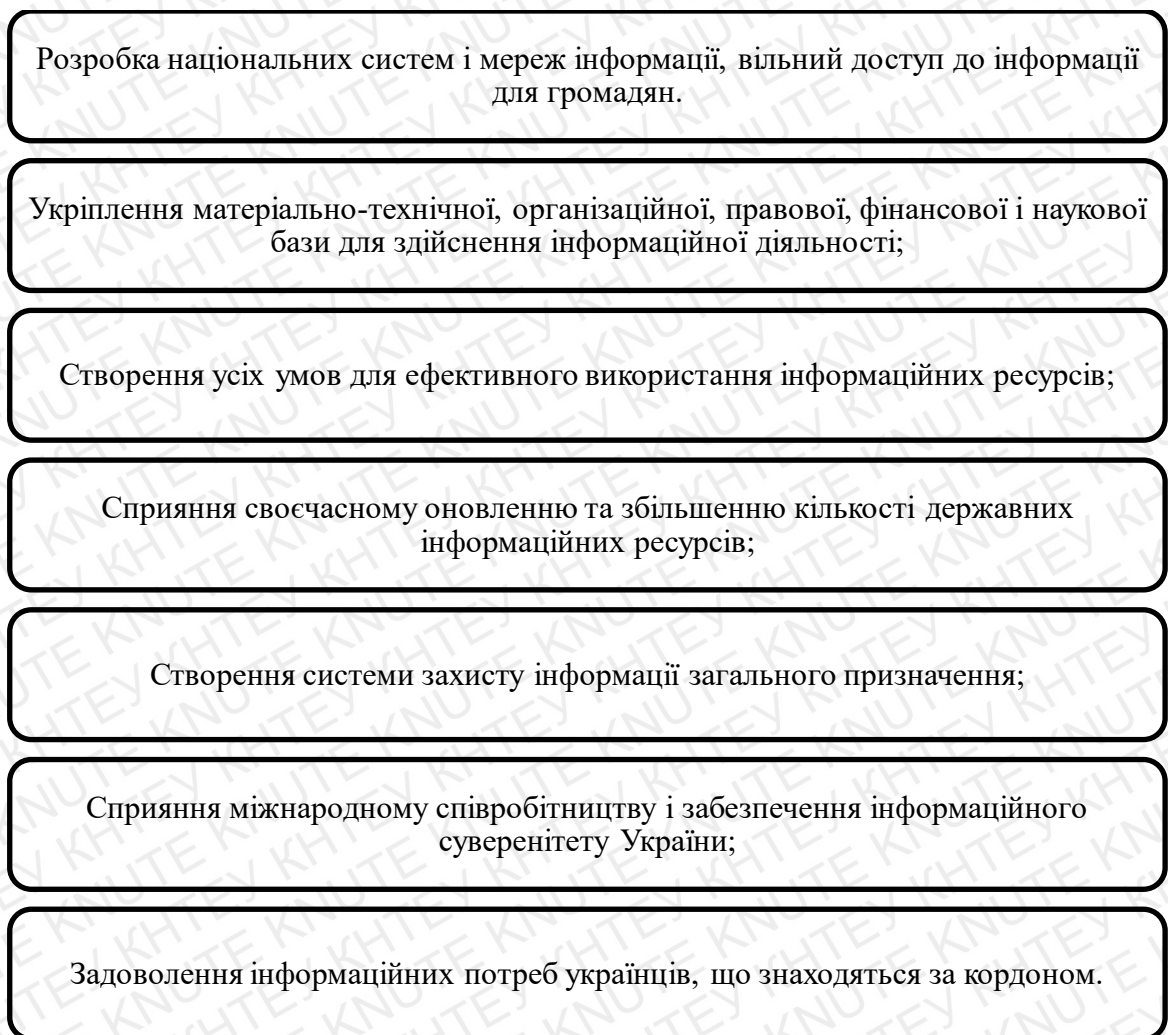
**Рис.2.1 Організаційно-правовий механізм захисту інформаційного простору України**

*Джерело:* побудовано автором за матеріалами[19]

Інформаційна політика держави являє собою сукупність способів і напрямів реалізації потужного комплексу взаємопов'язаних заходів правового та організаційного характеру, у результаті чого відбувається процес впливу уповноважених суб'єктів на об'єкти управління, з метою досягнення бажаного результату. В рамках реалізації державної інформаційної політики відбувається врегульована нормами права діяльність уповноважених на те суб'єктів, з метою втілення у життя різноманітних механізмів отримання, використання, поширення та зберігання інформації.[20]

Ефективність державної політики в інформаційній сфері залежить від вибору організаційно-правових інструментів і визначення напрямів діяльності.

Звернімо увагу на думку Ю. М. Іванченка, який висуває пропозицію виділити такі її головні напрями:[21]



**Рис.2.2 Напрями державної інформаційної політики**

*Джерело:* побудовано автором за матеріалами[21]

Ми погоджуємося з цією думкою, адже створення національних мереж інформації сприяє швидкому і надійному доступу до інформації для громадян та органів державної влади, а якісне впровадження таких систем є неможливим без дієвої системи захисту інформаційного простору.

Міжнародне співробітництво у галузі інформації гарантує появу перспектив щодо захисту прав громадян, які проживають на території України та за її межами на вільне використання та розповсюдження інформації.

Концепція державної інформаційної політики передбачала забезпечення дотримання норм суспільної моралі, в першу чергу, обмеження розповсюдження інформаційної продукції, здатної зашкодити людині і суспільству, зокрема щодо проявів нетерпимості, українофобії, антисемітизму, расизму, ксенофобії,



шовінізму, відповідно до закону, який є необхідним у демократичному суспільстві для забезпечення соціально-економічного зростання країни та для правового врегулювання злочинних дій в інформаційній сфері.

Ці питання і досі є актуальними, особливо ті, що стосуються сучасної українізації, зокрема питання української мови як державної. Мова є одним із основних чинників національної безпеки України, а це означає що законодавче закріплення її функціонування як державної стало ще одним правовим важелем впливу на формування інформаційного простору держави. Закон України «Про забезпечення функціонування української мови як державної» від 11.09.2020 р. забезпечує статус української мови як єдиної державної мови, передбачає обов'язковість її використання на всій території України при здійсненні повноважень органами державної влади та органами місцевого самоврядування, а також в інших публічних сферах суспільного життя[22].

У галузі державної безпеки необхідно забезпечити дієвий захист вітчизняної частини інтернет-простору та права журналістів, зокрема надання журналістам права не повідомляти про джерело інформації, крім законодавчо встановлених випадків, коли така інформація оприлюднюється за рішенням суду; недопускати прояви цензури та дій, які перешкоджають здійсненню журналістами їхньої професійної діяльності.

Діяльність журналістів в Україні регулюється Законом України «Про державну підтримку засобів масової інформації та соціальний захист журналістів», який гарантує права пільги та компенсацію за роботу із шкідливими та важкими умовами праці, охорону праці журналістів, на медичні огляди, соціальне страхування, на повне розслідування нещасних випадків, смерті і шкоди, яка була завданна здоров'ю журналіста при виконанні службових обов'язків. Згідно цього закону службова діяльність журналіста не може бути підставою для його затримання, арешту, а також вилучення опрацьованих, зібраних, підготовлених ним матеріалів та технічних засобів, які він використовує для виконання своєї роботи[23].

Наповнення інформаційного внутрішнього та зовнішнього інформаційного простору достовірною позитивною інформацією про Україну є надзвичайно важливим напрямом державної політики. В даному контексті важливим аспектом є підтримка ЗМІ, журналістів, які створюють якісний і достовірний контент, висвітлюючи основні події життя України.

В тому числі важливою є підтримка журналістів України, які живуть та працюють за її межами. Адже вони мають змогу розширювати межі інформаційного простору нашої держави та доповнювати його своєчасною інформацією про події, які відбуваються за кордоном, але мають важливе значення для нашої країни.

Підтримка так само є важливою збоку держави для тих медіа-продуктів на телебаченні та в соціальних мережах, які популяризують Україну за кордоном та слугують формуванню її позитивного іміджу, що дозволяє протидіяти руйнівному інформаційному впливу з боку країни-агресора.

Використання Російською Федерацією сучасних технологій гібридної війни для завдання шкоди Україні перетворило інформаційну галузь на головну платформу протиборства. Найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання релігійної, культурної та національної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності спрямовані саме на Україну.

Саме ці фактори спричинило розробки Доктрини інформаційної безпеки України затвердженої Указом Президента України 25 лютого 2017 р., основними завданнями якої є захист суспільства України від загарбницького впливу деструктивної пропаганди, розвиток медіа-культури суспільства і соціально відповідального медіа-середовища, забезпечення розвитку та функціонування української мови в усіх сферах суспільного життя та на всій території України, розвиток інформаційного суспільства, в тому числі його технологічної інфраструктури, а також розробка системи та механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, перш за все пропаганди[24].

Таблиця 2.1

**Аналіз національних інтересів України в інформаційній сфері і умов їх реалізації[24]**

| <b>Національні інтереси України в інформаційній сфері</b>                                                                                                                                     | <b>Умови їх реалізації за показником оперативного управління</b>                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Захищеність від деструктивних інформаційно-психологічних впливів                                                                                                                              | Передбачає виявлення та нейтралізацію цих впливів до того моменту, коли вони спричинять негативні наслідки.                                 |
| Захист українського суспільства від агресивного впливу пропаганди, передусім з боку Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі. | Передбачає постійний моніторинг інформаційного простору щодо виявлення загроз та безпосереднього негативного впливу, оперативне реагування. |
| Розвиток системи стратегічних комунікацій України.                                                                                                                                            | Створення системи, яка матиме активний інформаційний вплив, і включатиме інформаційні та психологічні операції.                             |
| Створення ефективних механізмів захисту інформаційного простору від негативних зовнішніх інформаційно-психологічних впливів, враховуючи у розробці норми міжнародного права.                  | Передбачає аналіз норм міжнародного права та моніторинг інформаційного простору щодо виявлення загроз та будь-якого негативного впливу.     |
| Формування позитивного іміджу України у світі, розповсюдження інформації про події в Україні до міжнародної спільноти.                                                                        | Чітко визначити, яка саме інформація є «оперативною» і налагодити міжнародні зв'язки.                                                       |
| Розвиток та захист національної інформаційної інфраструктури                                                                                                                                  | Передбачає моніторинг загроз та спроб впливу на функціонування інформаційної інфраструктури.                                                |



В. Гусаров, досліджуючи проблему інформаційної безпеки України, стверджує, що Росія здійснює інформаційно-психологічні атаки, щоб активізувати поширення конфлікту на сході України, здійснювати тиск на українське управління, щоб змусити його погодитись на російський сценарій урегулювання конфлікту. В. Гусаров виокремлює такі напрями інформаційно-психологічних атак проти України[25].

- нав'язування думки про неспроможність влади України керувати державою та приймати раціональні управлінські рішення;
- формування негативних суджень про воєнно-політичне керівництво України та про те, що хаотичні бойові дії призводять до невинуватених жертв серед сил АТО;
- поширення поглядів про те, що українська армія на Сході України деморалізована та неспроможна вести бойові дії, а також про недовіру особового складу до їхнього керівництва;

На нашу думку, перелік таких інформаційно-психологічних атак постійно збільшується. До них можна віднести: поширення неправдивої інформації про настрої жителів на непідконтрольних територіях, нівелювання фактів історії України, її державності та незалежності, спекулювання на релігійному питанні, що передбачає незадоволення влади Росії фактом набуття помісного статусу українським православ'ям, намагання вплинути на процеси державотворення через деякі політичні сили, нав'язування культурних цінностей за допомогою медіа-ресурсів.

Прямим доказом цього є те що у світовій базі даних EUvsDisinformation неодноразово були опубліковані російські фейки, в тому числі і ті, що стосуються агресії на Сході України. Пропагандистські російські ЗМІ найчастіше висвітлюють кілька версій подій, щоб ввести в оману громадян і спекулювати на тій, чи іншій темі в своїх інтересах.

Такий інформаційній експансії також сприяє недостатній професійний рівень українських виробників інформаційного продукту та послуг, його

неконкурентоздатність проявляється не лише на світовому ринку, а й в Україні і призводить до того, що українська аудиторія обирає альтернативні іноземні джерела інформації. Недостатній контроль з боку держави за дотриманням законів України політичними силами, представниками ЗМІ та окремими особами, які займаються підприємництвом в інформаційній сфері, є причинами того, що у наш час трапляються непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на дестrukцію моральних цінностей та свідомості українців[26].

До загроз національній безпеці України в інформаційній сфері потрібно зарахувати: несанкціоноване поширення інформації, викривлення, спотворення, блокування її, замовчування та упереджене висвітлення; прояви обмеження свободи слова та доступу громадян до інформації; інформаційну експансію з боку інших країн та деструктивне інформаційне втручання в інформаційний простір держави, що відбувається, коли країни з потужнішим інформаційним потенціалом мають змогу розширити свій вплив на населення та громадськість менш потужної країни, шляхом розповсюдження неприхованої дезінформації; поява і функціонування у національному інформаційному просторі держави неконтрольованих інформаційних потоків; недосконалість державної інформаційної політики та відсутність необхідної інфраструктури в інформаційній сфері; розміщення загальнодоступної дезінформації в Інтернеті; розповсюдження у ЗМІ культу жорстокості та насильства; повільне входження України у світовий інформаційний простір[27].

Отже, наявність суттєвих загроз інформаційній безпеці України є передумовою створення нових механізмів протидії негативним інформаційним впливам, в тому числі проявам інформаційної експансії з боку країни агресора, які є небезпечними не лише для інформаційного суверенітету, але і для територіальної цілісності країни.

## **2.2. Нормативно-правове регулювання захисту інформаційного простору в Україні**

В сучасних умовах високих темпів розвитку науково-технічного прогресу інформація стає важливим стратегічним елементом ресурсного потенціалу будь-якої держави. В процесі свого розвитку інформаційне суспільство постійно створює нові ресурси, а держава відповідно здійснює управління цими ресурсами.

Інформаційні дані перетворюються на інформаційні ресурси в той момент, коли їх залучено в процес регулювання спеціальних підсистем електронного урядування та коли їх починають використовувати для отримання конкретних результатів. Якщо розглядати ці ресурси через призму електронних даних, то інформаційні ресурси - це засоби управління та розвитку системи електронного уряду. Процес отримання та обміну інформацією забезпечується наявністю певних об'єктів та суб'єктів[28].

Термін «інформаційні ресурси» має широке тлумачення. Його зміст змінювався відповідно до когнітивних і практичних проблем кожної окремої галузі науки. Існує тенденція до розробки універсального визначення інформаційного ресурсу на нормативно-правовому рівні, але ця проблема ще не втратила своєї актуальності, оскільки жодне з існуючих сформульованих положень повністю не відображає всіх характерних ознак інформаційних ресурсів.

І.В. Мукамела вважає, що інформаційний ресурс являє собою об'ємну різнохарактерну і багатоаспектну сукупність відомостей про суб'єктів та об'єкти політики, про предметну сферу їх діяльності, тобто про різні, але взаємопов'язані процеси факти, події та явища, які служать вихідною інформацією для прийняття політичних рішень, а володіння інформаційними ресурсами є однією з найважливіших умов вибору найбільш оптимального способу дій в умовах складних соціальних процесів як на державному рівні, так і на світовій арені[29].

На думку, І.Л. Бачило і М.Юрайт інформаційні ресурси – це елемент, на основі якого утворюється система організації конкретної людської діяльності, у ході якої вхідний ресурс перетворюється на вихідний ресурс певної форми і



якості, відповідно до встановлених цілей діяльності. В основі цих процесів – обіг знань, які приймають доступну для використання форму – інформацію, далі вони акумулюються, узагальнюються, систематизуються за різними ознаками і оформлюються у вигляді інформаційних ресурсів [30].

Головною метою функціонування державних інформаційних ресурсів є задоволення інформаційних потреб громадян. Підвищити якість та швидкість обміну інформацією між державою і суспільством є застосування інформаційно-комунікаційних технологій. Формами надання інформаційних послуг державою є електронне інформування та електронне консультування. При чому електронне інформування є прикладом односторонньої комунікації між органами публічної влади, а консультування – двосторонньої.

Основою правового регулювання механізмів, які забезпечують ефективне функціонування державних інформаційних ресурсів є Положення про електронну взаємодію державних електронних інформаційних ресурсів, затверджене постановою Кабінету Міністрів України від 8 вересня 2016 р. № 606 «Деякі питання електронної взаємодії державних електронних інформаційних ресурсів». Це положення містить загальні засади здійснення обміну електронними даними, крім інформації, що становить державну таємницю, між суб'єктами владних повноважень з державних електронних інформаційних ресурсів під час надання адміністративних послуг та здійснення інших повноважень відповідно до покладених на них завдань.

У даному положенні термін «система електронної взаємодії державних електронних інформаційних ресурсів» тлумачиться як система призначена для автоматизації та технологічного забезпечення обміну електронними даними між суб'єктами владних повноважень з державних електронних інформаційних ресурсів під час надання адміністративних послуг та здійснення інших повноважень відповідно до покладених на них завдань шляхом використання відповідних сервісів, що є інтерфейсами прикладного програмування доступу до державних електронних інформаційних ресурсів, створеними згідно з єдиними

вимогами, а також шляхом використання єдиних протоколів, форматів, шаблонів довідників та класифікаторів [31].

Відповідно до даного Положення забезпечення електронної взаємодії відбувається за такими принципами (Рис 2.3.):



**Рис.2.3 Принципи електронної взаємодії**

*Джерело: побудовано автором за матеріалами [31].*

Постановою КМУ від 10 травня 2018 року «Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів» на законодавчому рівні прийнято Порядок організації електронної інформаційної взаємодії державних електронних інформаційних ресурсів. Відповідно до даного нормативно-правового акту постачальник і отримувач для здійснення електронної інформаційної взаємодії забезпечують встановлення так званого шлюзу безпечного обміну, розроблення веб-сервісу та веб-клієнта відповідно до регламенту роботи системи електронної взаємодії державних електронних інформаційних ресурсів, в якій шлюз безпечного обміну – це програмне забезпечення системи електронної взаємодії державних електронних

інформаційних ресурсів, що об'єднується із інформаційними системами отримувача і постачальника та використовує спеціальні засоби кваліфікованої електронної печатки [32].

Одним із цифрових механізмів, що забезпечують ефективне функціонування інформаційних ресурсів є система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта». Ця система являє собою сучасне організаційно-технічне рішення, яке дозволяє будувати безпечні інформаційні міжвідомчі взаємодії державним органам та органам місцевого самоврядування через Інтернет шляхом обміну електронними повідомленнями між їх інформаційними системами.

Цей ключовий елемент електронної інфраструктури України, учасниками якого є органи державної влади та місцевого самоврядування, забезпечує уніфікований доступ до державних реєстрів, що підвищує якість надання електронних публічних послуг громадянам та бізнесу.

Усі дані системи мають високий рівень захисту від негативних зовнішніх впливів, завдяки підписанню електронною печаткою та шифруванню всіх даних, які передаються, а також веденню протоколу подій, контролю доступу до веб-сервісів і реалізації заходів, спрямованих на протидію різноманітним атакам[33].

Згідно з результатами аналітичного дослідження «Стан та перспективи розвитку державних електронних інформаційних ресурсів», реалізованого за підтримки проекту міжнародної технічної допомоги «Прозорість та підзвітність у державному управлінні та послугах», який фінансують USAID та UKAID фінансова підтримка працездатності більшості державних реєстрів здійснюється за рахунок коштів державного бюджету, які розділяються наступним чином. (Рис. 2.4.)

Відповідно, найбільше коштів держава витрачає на апаратне забезпечення, захист інформації, модернізацію електронних систем та технічну підтримку, що, на нашу думку, є найважливішими складовими у якісному процесі обміну інформаційними ресурсами.





**Рис.2.4. Розподіл фінансування державних інформаційних ресурсів**

*Джерело: побудовано автором за матеріалами [34].*

У даному звіті також описано питання інтероперабельності державних ресурсів.

Інтероперабельність – функціональна сумісність, здатність до співпраці та взаємодії. Загалом це здатність програмних, програмно-апаратних продуктів різних виробників взаємодіяти і функціонувати між собою. Відповідно до Директиви Європейської комісії інтероперабельність може бути визначена як «можливість обміну інформацією та взаємного використання інформації, яка мається в результаті обміну» [35].

Основними проблемами на шляху до повноцінної інтероперабельності інформаційних ресурсів є такі: дублювання інформації, непрозорість сервісів

держави, що зумовлюють появу корупційних ризиків. Важливими проблемами є також узурпація державної інформації та відсутність оперативного доступу одного органу влади до інформації, яка належить іншому органу влади. В зв'язку з цим, підвищується трудомісткість і собівартість обслуговування державних реєстрів, а також зростає ймовірність занесення в державні реєстри недостовірної інформації, причиною цього є значний вплив людського фактора на забезпечення функціонування реєстрів.

Інформаційні ресурси є одним із основних інструментів прийняття ефективних управлінських рішень. Такі рішення приймаються шляхом обробки інформації, до яких входять етапи аналізу, розробки альтернатив і критеріїв вибору, які виконуються спеціалістами у функціональних підрозділах системи. Після процесу обробки інформація у вигляді готових варіантів рішень надходить керівнику, який уже приймає рішення. Керівник одноосібно, або з залученням інших відповідальних осіб здійснює вибір одного варіанта – остаточного рішення, яке безпосередньо стосується об'єкту управління і забезпечується необхідним владним впливом.

Державна політика у сфері формування інформаційних ресурсів та інформації має бути направлена на створення умов для ефективного та якісного інформаційного забезпечення управлінських рішень, які покликані вирішити стратегічні та оперативні завдання розвитку країни.

Державні інформаційні ресурси є складовою національних інформаційних ресурсів та мають споживчу цінність, а саме: політичну, економічну, освітню, наукову, оборонну, історичну та соціокультурну.

Будь який суб'єкт інформаційних відносин України, має право доступу до державних інформаційних ресурсів згідно політики безпеки та чинного законодавства, адже державні інформаційні ресурси – це результат інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства і держави, систематизовані та зафіксовані на матеріальних носіях інформації, як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні

ресурси, які проходять певну обробку й передаються у інформаційних системах державного і загального призначення, інші ресурси, що містять відомості, які є об'єктом права власності держави незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку і задоволення потреб громадян, суспільства, держави та підлягають захисту згідно визначеної політики безпеки й чинного законодавства[36].

Державні інформаційні ресурси можуть бути розділені на дві групи:

- інформаційні ресурси, призначені для вирішення завдань конкретного органу управління певної ланки;
- інформаційні ресурси, орієнтовані на зовнішнього користувача.

Останні формуються інформаційно-аналітичними структурами. Якщо вони мають загальне методичне керівництво, схожі завдання, які вирішуються на основі єдиних нормативних документів, то вони можуть бути названі державними інформаційними системами [37].

## **Висновки до розділу 2**

Отже, ефективність державної політики у сфері захисту інформаційного простору потребує створення сучасних інформаційних систем, а одним з основних напрямів державної інформаційної політики має стати налагодження механізмів забезпечення ефективного функціонування державних інформаційних ресурсів, що є базою для прийняття управлінських рішень. Швидкий доступ до інформаційних ресурсів держави та оптимізація їх використання залежить від якості інформаційних систем держави, що формуються на основі державних реєстрів.



### **РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В УКРАЇНІ ВІД ЗОВНІШНІХ ВПЛИВІВ**

#### **3.1. Обґрунтування необхідності створення ефективної системи захисту інформаційного простору, з метою забезпечення інформаційного суверенітету України**

Швидкий розвиток інформаційно-комунікаційних технологій та інтенсивне використання інформаційних ресурсів повинні забезпечуватися високим рівнем захисту інформації. Від ступеню захищеності інформації залежить стан однієї з основних складових національної безпеки – інформаційної безпеки.

Проблеми інформаційної безпеки в умовах глобальної інформатизації і розвитку Інтернету набувають стратегічного значення. Одним із головних завдань сучасної держави є гарантування інформаційної безпеки особистості, яка характеризується захищеністю її психологічного стану та свідомості від небезпечних інформаційних впливів, таких як маніпулювання, нав'язування, дезінформація та спонукування до образ[38].

Національний інформаційний простір України на даний момент підпадає під суттєві загрози та виклики, які можуть перешкоджати функціонуванню держави, її економічному та політичному розвитку, інтеграції у європейські структури. Загрози національній безпеці України в інформаційній сфері це – сукупність тих умов і чинників, що складають небезпеку інтересам громадян та національним інтересам, через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру загалом[39].

Забезпечення інформаційної безпеки держави порівняно нова державна функція, яка характеризується відсутністю сталих та визначених методів і механізмів, правового інструментарію їх реалізації. В умовах російсько-українського конфлікту захист національного інформаційного простору від негативних інформаційно-психологічних впливів війн і операцій, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого

значення та стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави.

На даний момент головною загрозою для інформаційного суверенітету України є інформаційна війна з боку Росії, що спрямована на різке нав'язування неправдивих фактів та стереотипів за допомогою ЗМІ та лідерів думок у соціальних мережах.

М. Маклюен вивів твердження, яке звучить так: “Істинно тотальна війна – це війна за допомогою інформації”. А, боротьба в інформаційній сфері має таку ж ціль, що і збройні конфлікти -економічна експансія та інші види агресивних впливів [40].

У книзі Д.М.Прокоф'єва «Інформаційна війна та інформаційна злочинність» наведено таке визначення: інформаційна війна – це дії, що були розпочаті для досягнення інформаційної переваги, завдаючи шкоду інформації та інформаційним системам супротивника при одночасному захисті власної інформації. Основні методи інформаційної війни – блокування та спотворення інформаційних потоків, які впливають на процес прийняття рішень[41].

Цілеспрямований інформаційний вплив на населення передбачає панівне становище суб'єкта інформаційної війни у всіх сферах життєдіяльності іншої держави: економічній, політичній, релігійній, психологічній, мистецькій, науково-технічній, а також міжнаціональних і міжнародних зв'язків. Зростання ефективності заходів інформаційної війни, досягається шляхом встановлення контролю над інформаційним простором іншої країни, цілеспрямованості і точності таких дій із урахуванням необхідного обсягу та рівня достовірної інформації, що доводиться, ступенем диференціації населення за системами матеріальних і духовних цінностей, здатності адекватно сприймати відомості та реагувати на них, а також політичної, економічної, етнічної та релігійної ситуації в державі чи регіоні [42].

Інформаційна війна проти України з боку Росії фактично ведеться ще з моменту проголошення незалежності України, проте значного впливу інформаційний простір зазнав з початком бойових дій на Сході країни.

Недостовірна інформація про події у нашій країні, яка поширюється в ефірах деяких російських телеканалів, завжди спрямована на дискредитацію України, розпалювання міжетнічної ворожнечі, закликів до ненависті, порушення суверенітету і територіальної цілісності, утвердження зверхності однієї нації над іншими. Через маніпулятивні матеріали завдається відчутна шкода споживачам інформації, іміджу України як держави, що стала на шлях євроінтеграції, порушується право людини на отримання якісного й безпечного телерадіопродукту[43].

Закріплення у медіасфері України з подальшою анексією частини національного інформаційного простору країна-агресор проводила комплексно. Поряд із покриттям власним сигналом прикордонних територій, свій продукт поширювала через супутниковий зв'язок, українських операторів кабельного ринку та увійшла з власним продуктом через регіональні телеканали[44].

Таким чином інформаційна війна, яка поєднує у собі усі види інформаційного протиборства є прямою загрозою інформаційному простору України. За песимістичним сценарієм результатом цієї війни може стати повна втрата інформаційного суверенітету, що може завдати непоправну шкоду національній безпеці країни.

В американському інформаційному просторі поширена така професія спін-доктора. Спеціалісти цієї сфери виправляють ситуації, які виникають через негативні інформаційні впливи, і надають їм потрібну форму для висвітлення у ЗМІ. Їх завдання полягає у тому, щоб бути активними та креативними інформаторами, а також впливати на розвиток подій в інформаційному просторі.

В той період, коли наша країна знаходиться у стані інформаційної війни, залучення експертів і така протидія інформаційній зброї є непоганою альтернативою для збереження своїх стійких позицій у сфері інформації.

Для того, що уникнути подальшого широкомасштабного маніпулювання свідомістю українців, потрібно розширювати методи протидії пропагандистським діям і підвищувати інформаційну культуру громадян, збільшуючи державну



частку у теле-та радіомовленні та посилюючи контроль над інформацією, що публікується у Інтернет-джерелах.

До виявів інформаційної війни може бути зарахована й так звана інформаційна злочинність, велика частка якої припадає на кіберзлочини. Враховуючи сучасні тенденції до розширення мережевої архітектури організованої злочинності, в наш час формуються неформальні групи хакерів у віртуальному просторі. Також наявна інформація про залучення організованими групами кібер-злочинців до підготовки злочинів у кредитно-банківській сфері, на фондовому ринку, до протиправного отримання службової інформації. Не виключена й розробка організованими злочинними співтовариствами планів інформаційних диверсій[45].

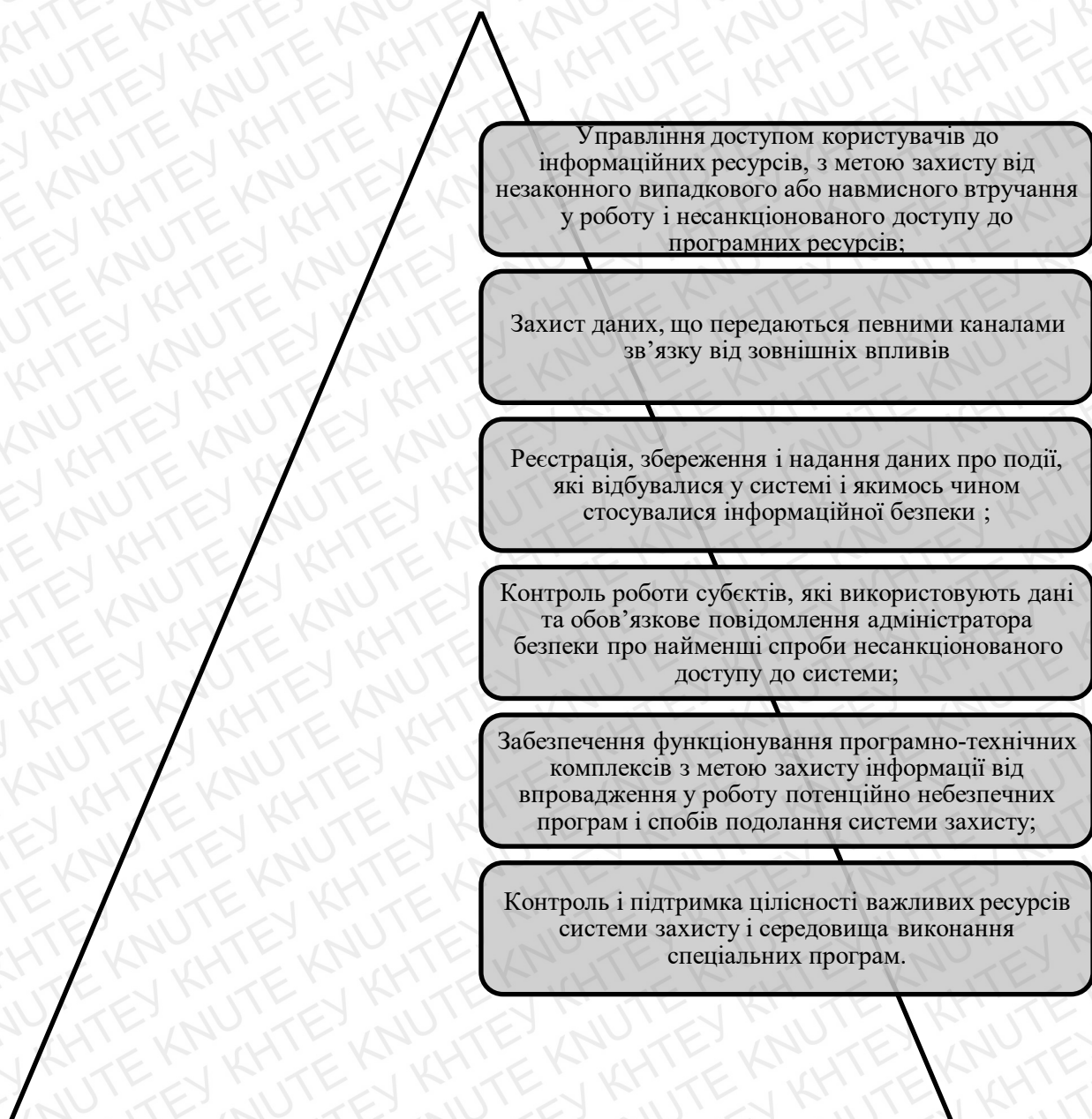
Різні індикатори реалізованих заходів у сфері захисту комп'ютерних та телекомунікаційних мереж від кібератак і створення умов для безпечного функціонування кіберпростору оцінюються та використовуються для моніторингу і порівняння стану кібербезпеки різних країн світу у щорічних міжнародних рейтингах, найбільш авторитетними з яких є Global Cybersecurity Index. Рейтинг країн Global Cybersecurity Index 2018 наведено у Додатку А.

Відповідно до результатів Global Cybersecurity Index 2018 Україна посіла 54 місце серед 193 країн, підвищила свій результат на 5 позицій та отримала схвальні відгуки від експертів щодо побудови законодавчої бази для гарантування кібербезпеки держави, стійкості державних ініціатив щодо підвищення кібербезпеки у сфері інформаційно-комунікаційних технологій і покращенню кіберстійкості організацій за останній рік, незважаючи на збільшення цілеспрямованих кібератак[46].

Проведення моніторингу кібератак та підвищення рівня обізнаності щодо кіберпростору є важливими елементами захисту інформації, тому у світі з'являються різноманітні ресурси для відслідковування кібератак, одним із них є онлайн-ресурс Security Tachometer, розроблений найбільшою в Європі телекомунікаційною компанією Deutsche Telekom. Цей портал дозволяє в

реальному часі побачити кібератаки і країни їх походження, а також перелік регіонів з найбільшою кількістю сервісів, які здійснюють такі атаки (Додаток Б).

Концепція технічного захисту інформації в Україні, яка є складовою забезпечення національної безпеки України передбачає такі завдання у сфері захисту інформації (Рис 3.1.):



**Рис.3.1. Завдання України у сфері захисту інформації**

*Джерело: побудовано автором за матеріалами [47].*

Концепція технічного захисту інформації визначає базу для створення комплексу заходів щодо інформаційної безпеки, передбачаючи необхідні, конкретні засоби захисту, які є найбільш дієвими з точки зору наявних інформаційних, фінансових та людських ресурсів [47].

Технології захисту даних базуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті. Сьогодні використовуються такі основні методи захисту інформації (Рис. 3.2.):



**Рис.3.2. Основні методи захисту інформації**

*Джерело:* побудовано автором за матеріалами[47].

У Стратегії національної безпеки України підкреслено, що загрози інформаційній безпеці окрім інформаційної війни проти України та відсутності цілісної політики у сфері захисту інформації складає недостатній рівень медіа-культури суспільства, що є ще одним підтвердженням необхідності створення ефективної системи захисту інформаційного простору.



У сучасних реаліях медіа-простір формує віртуальну реальність, яка активно програмує свідомість і поведінку людей. До прикладу, різка диференціація медіа-споживання у різних регіонах нашої країни, спричинена переважанням тих чи інших інформаційних каналів, може стати загрозою не лише для інформаційного простору країни, але і для цілісності її території.

Медіа-простір зазнає постійних змін та перетворень у цілому і в окремих складових частинах. Цей процес має внутрішньо суперечливий характер через взаємодію в ньому тенденцій стандартизації та індивідуалізації споживання інформації, глобалізації, пов'язаної з розширенням аудиторії, та спеціалізації аудиторії за інтересами.

Поява альтернативної медіа-культура розкриває нові можливості для розвитку суспільства. Відхід від «масовості» та однотипного споживацького конвеєра має змінитися на користь критичного і більш раціонального підходів до процесу сприйняття інформації у глобальному світі. Той факт, що люди часто сприймають інформацію з одних і тих самих джерел і ніколи не піддають її сумніву можна викорінювати спонуканням громадян до критичного та інтелектуального осмислення усіх інформаційних потоків [48].

Оскільки від рівня медіа-культури в країні залежить загальне налаштування населення, то укріплення позицій уже існуючих та поява нових альтернативних медіа-джерел, які покликані транслювати національно-патріотичні думки, сприяти українізації та культурному збагаченню національного медіа-простору. Це дозволить зменшити вплив пропаганди з боку країни агресора на свідомість громадян України.

### **3.2. Шляхи вдосконалення механізму захисту інформаційного простору**

#### **України від зовнішніх впливів**

На сьогоднішній день посилюється увага до вирішення одного з найважливіших завдань сучасного суспільства – створення безпечного інформаційного простору. Захист інформації відбувається шляхом розробки та реалізації діючих організаційно-правових механізмів.

Оскільки однією з основних загроз інформаційного простору України нами було визначено інформаційну війну, яка ведеться Росією проти української державності, то важливо визначити шляхи вдосконалення заходів органів державної влади, які будуть направлені на вирішення саме цієї проблеми.

На основі принципу інтероперабельності необхідно створити тісну систему взаємодії між усіма органами влади, які забезпечують інформаційну безпеку країни. Шляхом внесення змін до законодавства, розробити систему заходів, спрямованих на обмеження російського впливу та розповсюдження неправдивої і антиукраїнської інформації в усіх регіонах України, особливо прикордонних. Першочерговим також є сприяння створенню новим національним інформаційним продуктам, метою яких буде патріотичне виховання молоді та позиціонування України, як сильної та незалежної держави.

Забезпечення захисту інформаційного простору України лежить в основі завдань законодавчої, виконавчої влади та Президента України, від повноти виконання яких залежить стан інформаційної безпеки України.

Стратегічний рівень інформаційної безпеки забезпечує Верховна Рада України. Саме цей орган влади розробляє правові засади функціонування системи, що забезпечує національну безпеку в інформаційній сфері, затверджує порядок створення та повноваження Ради національної безпеки і оборони України, здійснює законодавче регулювання політики у цій сфері. Поруч з тим Верховна Рада України виконує не у повному обсязі або взагалі не виконує такі завдання як: реалізація загальнодержавної програми захисту інформаційного простору України та контролювання ходу її виконання, затвердження бюджетних асигнувань для фінансування діяльності щодо забезпечення національної безпеки в інформаційній сфері.

Президент України здійснює загальне керівництво у сфері інформаційної безпеки України, а саме: є головою Ради національної безпеки і оборони України, здійснює керівництво в інформаційній та інших сферах національної безпеки та оборони України, забезпечує взаємодію виконавчої, законодавчої та судової

гілок державної влади між собою, а також із недержавними організаціями, які забезпечують національну безпеку в інформаційній сфері.

Поруч з тим, Президентом України виконуються не в повній мірі або взагалі не виконуються такі повноваження: звітування перед народом України про стан національної безпеки України раз на рік на сесії Верховної Ради, визначення уже існуючих і потенційних загроз та небезпек для національної безпеки в інформаційній сфері та вживання усіх необхідних заходів із забезпечення захисту інформаційного простору та здійснення контролю і координації діяльності державних органів у забезпеченні національної безпеки в інформаційній сфері.

Кабінет Міністрів України забезпечує інформаційний суверенітет України, здійснює внутрішню і зовнішню інформаційну політику держави, реалізовує заходи щодо забезпечення прав і свобод людини і громадянина в інформаційній сфері, визначає обсяг фінансових ресурсів на забезпечення інформаційної безпеки, забезпечує виконання затвердженого Верховною Радою України Державного бюджету України щодо фінансування заходів у сфері інформаційної безпеки у визначених обсягах. В той же час КМУ не в повній мірі організовує розроблення і виконання державних програм та проектів з розвитку інформаційної інфраструктури органів державного управління.

Міністерства та інші центральні органи виконавчої влади виконують такі повноваження: забезпечують реалізацію законів України, указів та розпоряджень Президента України, концепцій, доктрин, програм, постанов органів державного управління; управляють діяльністю підвідомчих організацій з планування і проведення заходів щодо забезпечення інформаційної безпеки, забезпечують застосування інструментів та засобів забезпечення інформаційної безпеки, а також управління їх діяльністю. Але поруч з тим не виконують такі завдання, як: притягнення до відповідальності посадових осіб, дії яких призводять до порушення національних інтересів в інформаційній сфері, створюють безпосередню загрозу інформаційній безпеці України [49].

З метою формування ефективного, надійного і безпечного інформаційного простору України, слід також сфокусуватись на зміцненні національного науково-



виробничого потенціалу інформатизації, телекомунікацій і зв'язку, виробництві інформаційного продукту та ефективної системи надання різних інформаційних послуг користувачам, у першу чергу, громадянам. Необхідно також забезпечити реформування інформаційного забезпечення в системі органів державної влади [50].

Правове регулювання в інформаційній сфері має не лише відповідати сучасним реаліям, а й має вирішувати суперечність між потребами особи, суспільства та держави у вдосконаленні процесів вільного обміну інформацією та обмеженнями на поширення окремих відомостей. Особливої уваги вимагає законодавство про засоби масової інформації, законодавство про формування інформаційних ресурсів, законодавство про інформаційну та кібернетичну безпеку; законодавство про порядок реалізації права на пошук, отримання, передачу та використання інформації, а також необхідним є створення широкого спектру інформаційних продуктів, надання інформаційних послуг[51].

Шаповал Р.В та Ключко В.О. вважають, що вдосконалення нормативно-правового забезпечення, попередження й нейтралізація потенційних і реальних загроз національній безпеці в інформаційній сфері потребує розроблення концептуальних основ забезпечення інформаційної безпеки. Це важлива умова удосконалення адміністративно-правового регулювання відносин у сфері захисту національних інтересів, утвердження України як суверенної і незалежної, демократичної, соціальної, правової держави та її політико-правового позиціонування у світовому просторі[52].

Ми погоджуємося з цією думкою і вважаємо, що при вдосконаленні концептуальних засад захисту інформаційного простору наша країна зможе укріпити свої позиції на міжнародному рівні, що дасть змогу швидше і якісніше виявляти зовнішні загрози національній безпеці і долати їх, заручившись підтримкою інших держав.

На державному рівні захист інформації здійснюється за чітко визначеними напрямками організаційно-правового забезпечення(Рис. 3.3.).



**Рис.3.3 Напрями організаційно-правового забезпечення захисту інформаційного простору**

*Джерело:* побудовано автором за матеріалами [53].

В.Т. Колесник вважає, що забезпечити розвиток національної індустрії інформації, збереження і захист інформаційних ресурсів потребує розробки нових організаційних можливостей для боротьби з загрозами у кіберпросторі, а саме впровадження єдиної національної стратегії із кібербезпеки.

Наступним кроком має стати створення і активне використання інноваційних автоматизованих систем та мереж для передачі даних, а також посилення заходів захисту, які направлені на виявлення і нейтралізацію усіх загроз в режимі реального часу[54].

Таким чином Ткачук Т.Ю. розглядає захист інформаційного простору України, як діяльність, яка здійснюється у таких напрямках як захист

першочергових інтересів особистості, суспільства та держави від усіх імовірних загроз та захист інформаційного суверенітету України.

Першочерговими заходами захисту інтересів особистості, суспільства і держави є такі:

- покращення діючої системи засобів інформаційного протиборства Збройних сил України, військових об'єднань та органів спеціального призначення;
- імплементація ефективних механізмів передбачення та моніторингу інформаційних загроз;
- знищення інформаційно-психологічного впливу, в тому числі спрямованого на викривлення історичних фактів та підлив національної свідомості;
- розповсюдження національного інформаційного продукту на тимчасово непідконтрольних територіях України, впровадження системного підходу до державної інформаційної політики цих територій;
- підвищення рівня інформаційної культури та культури особистої інформаційної безпеки, реалізація запобіжних заходів щодо правопорушень в інформаційній сфері.

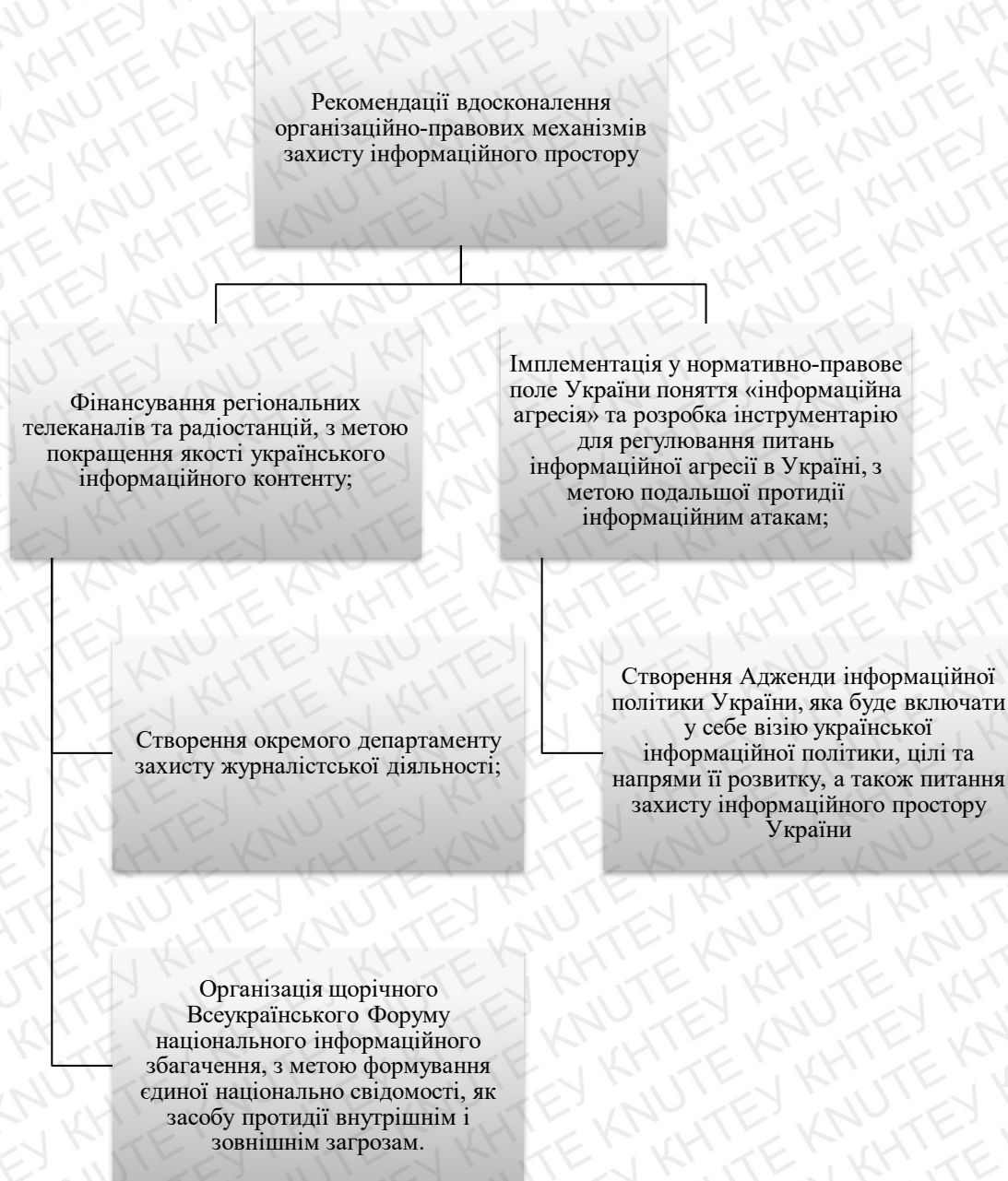
Підтримка економічно-соціальної та політичної стабільності, територіальної цілісності України та захист національного інформаційного суверенітету передбачає такі заходи:

- протидія застосуванню інформаційних технологій для пропаганди міжособистісної ворожнечі громадян всередині країни та поширення екстремістських поглядів;
- забезпечення захисту державної таємниці та інформації з обмеженим доступом військово-промислових підприємств.
- протидія інформаційному впливу, спрямованому на знищення духовних та культурних цінностей українського народу;
- розробка державних освітніх програм підготовки спеціалістів з протидії негативним інформаційним впливам[55].



Зміст інформаційної безпеки передбачає не лише стан захищеності, а й створення усіх умов, які сприятимуть розвитку інформаційного простору.

В результаті наших досліджень ми пропонуємо перелік рекомендацій для Міністерства культури та інформаційної політики, спрямовані на вдосконалення організаційно-правових механізмів захисту інформаційного простору від зовнішніх впливів (Рис.3.4).



**Рис.3.4 Рекомендації щодо вдосконалення організаційно-правових механізмів**

*Джерело:* Розроблено і побудовано автором.

### **Висновки до розділу 3**

Отже, до основних шляхів вдосконалення організаційно-правового забезпечення у сфері захисту інформаційного простору в Україні можна віднести модернізацію законодавчої бази, яка буде відповідати сучасним реаліям, реалізація ефективної державної політики у сфері інформації та приведення у дію усіх елементів організаційно-правових механізмів, передбачених законодавством у сфері інформаційної безпеки. Організаційну складову можна підсилити шляхом розвитку національної інформаційної інфраструктури, в тому числі державної теле та радіомереж, а також вдосконалення механізмів взаємодії органів державної влади та інститутів громадянського суспільства.

## ВИСНОВКИ

У сучасних реаліях захист інформаційного простору України від негативних інформаційних проявів набуває особливої важливості.

У роботі визначено сутність понять «інформаційний простір» та інформаційна безпека». Інформаційний простір країни являє собою сукупність усіх інформаційних потоків національного та іноземного походження, які доступні на території держави. Інформаційна безпека – це стан захищеності інформаційної інфраструктури держави. Поняття інформаційного простору нерозривно пов'язано з поняттям інформаційної безпеки.

Визначено основні проблеми захисту інформаційного простору України, зокрема такі: використання засобів масової інформації окремими політичними силами; некомпетентність працівників державних органів і установ; вплив на засоби масової інформації організованої злочинності; недостатня інтегрованість України у світове інформаційне поле та інші.

Проаналізовано нормативно-правове забезпечення в інформаційній сфері. До нормативно-правових актів, які регулюють систему забезпечення інформаційної безпеки в Україні належать: Конституція України, закони України «Про основи національної безпеки України», «Про інформацію», «Про Концепцію Національної програми інформатизації», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення та радіомовлення», «Про інформаційні агентства», «Про державну таємницю», «Про державну підтримку засобів масової інформації та соціальний захист журналістів» та іншими нормативно -правовими актами.

Досліджено стан організаційно-правових механізмів державної політики в інформаційній сфері. Існуючі організаційно-правові механізми потребують вдосконалення, адже вони не враховує усі актуальні аспекти інформаційної боротьби ХХІ століття.

Визначено основні напрями державної інформаційної політики в Україні, а саме: сприяння постійному оновленню та ефективному використанню



національних інформаційних ресурсів, створення загальної системи захисту інформаційного простору, забезпечення доступу громадян до інформації, шляхом створення національних мереж інформації, сприяння міжнародному співробітництву в галузі інформації та інші.

Проаналізовано основні механізми, що забезпечують ефективне функціонування інформаційних ресурсів держави. Приміром, застосування інформаційно-комунікаційних технологій підвищують якість та швидкість обміну інформаційними ресурсами між державою і суспільством, а використання інструментів електронної взаємодії забезпечує безпечність цього обміну.

Визначено основні загрози інформаційній безпеці України. На даний момент головними загрозами для інформаційного суверенітету України є інформаційна війна з боку Росії, кіберзлочинність та недостатній рівень медіа-культури суспільства. Підвищення рівня інформаційної культури дозволить зменшити негативний вплив на свідомість громадян з боку країни-агресора і дасть змогу створити ефективну систему захисту інформаційного простору.

Розроблено рекомендації щодо шляхів вдосконалення організаційно-правового забезпечення у сфері захисту інформаційного простору України, а саме: збільшення фінансування регіональних ЗМІ, з метою покращення якості інформаційного медіа-контенту, створення окремого департаменту захисту журналістської діяльності, імплементація у нормативно-правове поле України поняття «інформаційна агресія» та розробка інструментарію для регулювання проявів інформаційної агресії, створення Адженди інформаційної безпеки України, а також започаткування щорічного Всеукраїнського Форуму національного інформаційного збагачення.

Отже, на сьогодні питання захисту інформаційного простору від зовнішніх впливів є важливою складовою національної безпеки країни. В умовах інформаційної війни та недостатнього рівня інформаційної культури у суспільстві, вдосконалення організаційно-правових механізмів захисту інформаційного простору України є першочерговим завданням для збереження інформаційного суверенітету України.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гурковський В. І. Захист іміджу Української держави в умовах інформаційної глобалізації / В. І. Гурковський. // Державне управління: теорія та практика. - 2012. - № 2. - Режим доступу: [http://nbuv.gov.ua/UJRN/Dutp\\_2012\\_2\\_11](http://nbuv.gov.ua/UJRN/Dutp_2012_2_11)
2. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / В. М. Фурашев // Інформація і право. - 2012. - № 2. - С. 162-169. - Режим доступу: [http://nbuv.gov.ua/UJRN/Infpr\\_2012\\_2\\_24](http://nbuv.gov.ua/UJRN/Infpr_2012_2_24)
3. Лобузінa, Катерина Вілентіївна. Створення інтегрованого бібліотечного простору: основні проблеми та шляхи вирішення / К. В. Лобузінa // Бібліотекознавство. Документознавство. Інформологія. – 2012. – № 2. – С. 34-40. ) - [Електронний ресурс]. – Режим доступу: –<http://irbis-nbuv.gov.ua/everlib/item/er-0000000022>
4. Макаренко Є. А. Європейська інформаційна політика / Є. А. Макаренко. – К.: Наша культура і наука. 2000. – 368 с
5. Концепція інформаційної безпеки України (Проект) - [Електронний ресурс]. – Режим доступу: <https://www.osce.org/uk/fom/175056?download=true>
6. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: монографія / Б. А. Кормич. – Одеса: Юридична література, 2003. – 472 с.
7. Сорокін О. Л. Інформаційна безпека та її складові: проблеми визначення концепту / О. Л. Сорокін // Держава та право. – 2014. – №8. – С. 18-22.
8. Громико І., Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам / І. Громико, Т. Саханчук. // Право України. – 2008. – № 8.

9. Доктрина інформаційної безпеки України: Затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. - [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua/laws/show/47/2017?lang=ru>.
10. Бондаренко В., Литвиненко О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. Бондаренко, О. Литвиненко - Режим доступу: <http://www.crime-research.iatr.org.ua/library/strateg.htm>.
11. Закон України «Про інформацію» - [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12>
12. Закон України “Про основи національної безпеки України” - [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/964-15>
13. Рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28.04.2014 року - [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/n0004525-14>
14. Інформація з офіційного веб-сайту Міністерства інформаційної політики України - [Електронний ресурс]. – Режим доступу <http://mip.gov.ua/>.
15. Питання діяльності Міністерства інформаційної політики України. - [Електронний ресурс]. – Режим доступу <http://zakon3.rada.gov.ua/laws/show/2-2015-%D0%BF>.
16. Інформаційна безпека як основа національної безпеки / І. Р. Боднар // Mechanism of Economic Regulation. - 2014. - № 1. - С. 68-75. - Режим доступу: [http://nbuv.gov.ua/UJRN/Mre\\_2014\\_1\\_8](http://nbuv.gov.ua/UJRN/Mre_2014_1_8)
17. Небога І. Теоретичні основи формування системи захисту інформаційного простору України / І. Небога // Публічне управління та адміністрування в умовах суспільних трансформацій : зб. наук. ст. студ. відп. ред. Н.Л. Новікова. – К.: Київ. нац. торг.-екон. ун-т, 2020. – 251 с., С. 168-174.



18. Красноступ Г.М. Основні напрями правового забезпечення державної інформаційної політики / Г.М. Красноступ // Офіційний веб-сайт Міністерства юстиції України [Електронний ресурс]. – Режим доступу: <http://old.minjust.gov.ua/30768>
19. Антонюк В.В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці / В.В. Антонюк // Державне управління: удосконалення та розвиток. — Вип. 8 (10). — 2014. — С. 1—5. - [Електронний ресурс]. — Режим доступу: <http://www.dy.nayka.com.ua/?op=1&z=747>
20. Негодченко, В. Основні напрями державної інформаційної політики в Україні [Електронний ресурс] / В. Негодченко. - Електрон. текстові дан. // Підприємництво, господарство і право : науково-практичний господарсько-правовий журнал. До 2001 г. виходив російською мовою. - 2016/1. - № 4. - С. 77-81. - [Електронний ресурс]. — Режим доступу: [http://nbuv.gov.ua/UJRN/Pgip\\_2016\\_4\\_15](http://nbuv.gov.ua/UJRN/Pgip_2016_4_15)
21. Іванченко Ю.М. Сутність, головні напрями та способи державної інформаційної політики в Україні / Ю.М. Іванченко // Державне управління: теорія та практика. – 2005. – № 2 [Електронний ресурс]. – Режим доступу : <http://www.academy.gov.ua/ej/ej2/>:
22. Закон України «Про забезпечення функціонування української мови як державної» - [Електронний ресурс]. — Режим доступу: <https://zakon.rada.gov.ua/laws/show/2704-19#Text>
23. Закон України «Про державну підтримку засобів масової інформації та соціальний захист журналістів» - [Електронний ресурс]. — Режим доступу: <https://zakon.rada.gov.ua/laws/show/540/97-%D0%B2%D1%80#Text>
24. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» - [Електронний ресурс]. — Режим доступу: <https://zakon.rada.gov.ua/laws/show/47/2017#Text>

25. Тези доповідей Всеукраїнської науково-практичної конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів "Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка" [Текст] / за заг. редакцією І.В. Толока. – К. : ВІКНУ, 2019. – 344 с. – [Електронний ресурс]. – Режим доступу: [https://mil.univ.kiev.ua/files/255\\_1385750646.pdf](https://mil.univ.kiev.ua/files/255_1385750646.pdf)
26. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: <http://www.justinian.com.ua/article.php?id=322214>
27. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / У. Ільницька // Humanitarian vision. - 2016. - Vol. 2, Num. 1. - С. 27-32. [Електронний ресурс] - Режим доступу: [http://nbuv.gov.ua/UJRN/hv\\_2016\\_2\\_1\\_7](http://nbuv.gov.ua/UJRN/hv_2016_2_1_7)
28. Приймак Ю.Ю. Національні інформаційні ресурси – джерело державних інформаційних продуктів та послуг // Державне управління : теорія та практика. – 2009. – № 2.- [Електронний ресурс]. – Режим доступу: [http://academy.gov.ua/ej/ej10/doc\\_pdf/Priymak.pdf](http://academy.gov.ua/ej/ej10/doc_pdf/Priymak.pdf)
29. Мукомела І. В. Інформаційні ресурси та їх вплив на державно-правовий розвиток / І. В. Мукомела // Державне будівництво та місцеве самоврядування. - 2013. - Вип. 26. - С. 190-202. [Електронний ресурс]. - Режим доступу: [http://nbuv.gov.ua/UJRN/dbms\\_2013\\_26\\_17](http://nbuv.gov.ua/UJRN/dbms_2013_26_17)
30. Інформаційне право: актуальні проблеми теорії та практики: монографія / за заг. Ред. І. Л. Бачило. - М.: Юрайт, 2009. – с.530
31. Постанова Кабінету Міністрів України №606 від 8 вересня 2016 р.«Деякі питання електронної взаємодії державних електронних інформаційних ресурсів» - [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/606-2016-%D0%BF#Text>
32. Постанова Кабінету Міністрів України №357 від 10 травня 2018 р. «Деякі питання організації електронної взаємодії державних електронних

інформаційних ресурсів» [Електронний ресурс]. – Режим доступу: <https://ips.ligazakon.net/document/view/kp180357?an=90>

33. Офіційний сайт системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» - [Електронний ресурс]. – Режим доступу: <https://trembita.gov.ua/ua/projects/trembita-vzayemodiya-reyestriv>

34. Звіт за результатами аналітичного дослідження «Стан та перспективи розвитку державних електронних інформаційних ресурсів - [Електронний ресурс]. – Режим доступу: [http://tapas.org.ua/wpcontent/uploads/2018/11/Report\\_SEIR\\_UKR.pdf](http://tapas.org.ua/wpcontent/uploads/2018/11/Report_SEIR_UKR.pdf)

35. Мартиненко С.В . Про інтероперабельність та безпеку Національної системи електронних цифрових підписів в Україні // -2011. –с.30 - [Електронний ресурс]. – Режим доступу: [http://www.itsway.kiev.ua/pdf/About\\_interoperability.pdf](http://www.itsway.kiev.ua/pdf/About_interoperability.pdf)

36. Юдін О.К., Бучик С.С. Концептуальний аналіз уразливості державних інформаційних ресурсів // Наукоємні технології. – 2013. – № 3(19). – (Технічні науки). – С. 299-304.

37. Довгань О. Д. Інформаційні ресурси: національні та державні, зміст, поняття / О. Д. Довгань // Інформація і право. - 2015. - № 3. - С. 85-91. - [Електронний ресурс]. - Режим доступу: <http://ippi.org.ua/sites/default/files/dovgan.pdf>

38. Я. Жарков. Небезпеки особистості в інформаційному просторі. Розділ І. Аналітика. Інформаційна безпека. “Юстініан”. – 2007. №2. . - [Електронний ресурс]. - Режим доступу: <http://www.justinian.com.ua/article.php?id=2554>

39. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: <http://www.justinian.com.ua/article.php?id=3222>

40. McLuhan, M. Understanding Media; McGraw Hill: New York, NY, USA. - [Електронний ресурс]. – Режим доступу:



<https://designopendata.files.wordpress.com/2014/05/understanding-media-mcluhan.pdf>

41. Сливка В. Інформаційна війна проти України: міф чи реальність? - [Електронний ресурс] / В. Сливка. – Режим доступу <http://intkonf.org/slivka-vv - informatsiyna-viyna-proti-ukrayini-mif-chi-realnist/>
42. Малик Я. Й. Інформаційна війна і Україна / Я. Й. Малик. // Демократичне врядування. - 2015. - Вип. 15. - [Електронний ресурс]. – Режим доступу: [http://lvivacademy.com/vidavnitstvo\\_1/visnyk15/fail/Malyk.pdf](http://lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf)
43. Звіт Національної ради України з питань телебачення і радіомовлення за 2014 рік [Електронний ресурс]. – Режим доступу : <http://nrada.gov.ua/ua/zvitnainformacia/zvitnatsrady/21901.html>.
44. - [Електронний ресурс]. – Режим доступу: <file:///C:/Users/User/Downloads/679-1921-1-SM.pdf>
45. Ткачук Т.Ю. Сучасні загрози інформаційній безпеці держави:теоретико-правовий аналіз/ Т.Ю. Ткачук. // Підприємництво, господарство і право.- 2017. - Вип.10.- [Електронний ресурс]. – Режим доступу: <http://pgp-journal.kiev.ua/archive/2017/10/38.pdf>
46. Моніторинг рівня кібербезпеки України у світових рейтингах / Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. // Інформаційна безпека людини, суспільства, держави. – Київ: Національна академія Служби безпеки України. – 2019. – №3(27). – С. 100–107.- [Електронний ресурс]. – Режим доступу: [http://www.academy.ssu.gov.ua/ua/page/page\\_1581429315.htm](http://www.academy.ssu.gov.ua/ua/page/page_1581429315.htm)
47. Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» - [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text>
48. Різун В. В. Теорія масової комунікації. Підручник. – К.: Просвіта, 2008. – 260 с.- [Електронний ресурс]. – Режим доступу: <http://filelibsnu.at.ua/navchalno-metod/jurnalistika/Teoriya mas com.pdf>

49. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання [Текст] : монографія / А.Ю. Нашинець-Наумова. – Київ: «Гельветика», 2017. – 168 с.- [Електронний ресурс]. – Режим доступу: [http://elibrary.kubg.edu.ua/id/eprint/18860/1/A\\_Nashinets-Naumova\\_monografia\\_1\\_FPMV.pdf](http://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_monografia_1_FPMV.pdf)
50. Гіда О.Ф. Щодо основних засад формування державної інформаційної політики /О.Ф.Гіда.- Боротьба з організованою злочинністю (теорія і практика), №1 (29) 2013. – С.333-341.- [Електронний ресурс]. – Режим доступу: [file:///C:/Users/User/Downloads/boz\\_2013\\_1\\_40.pdf](file:///C:/Users/User/Downloads/boz_2013_1_40.pdf)
51. Форос Г.В. Правові основи захисту інформації в кіберпросторі/ Правова держава. 2018 -Вип.№30.с.181-186.-[Електронний ресурс]. – Режим доступу: <file:///C:/Users/User/Downloads/132891-299998-1-PB.pdf>
52. Шаповал Р.В., Клочко В.О. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України/ Р.В. Шаповал, В.О. Клочко// Наше право.- 2014.-Вип.6.- с.5-9.- [Електронний ресурс]. – Режим доступу: [file:///C:/Users/User/Downloads/Nashp\\_2014\\_6\\_3%20\(3\).pdf](file:///C:/Users/User/Downloads/Nashp_2014_6_3%20(3).pdf)
53. Логінова, Наталія Іванівна.Правовий захист інформації [Текст] : навч. посіб. / Н. І. Логінова, Р. Р. Дробожур ; Нац. ун-т "Одес. юрид. акад.", Каф. інформ. технологій. - Одеса : Фенікс, 2015. - 262- [Електронний ресурс]. – Режим доступу: <https://cutt.ly/ig1wJNO>
54. Колесник В.Т. Розвиток та удосконалення організаційно-правових механізмів державного управління у сфері забезпечення національної безпеки України/ В.Т.Колесник//Державне управління:удосконалення та розвиток.-2015.-Вип.№12.- [Електронний ресурс]. – Режим доступу: <http://www.dy.nayka.com.ua/?op=1&z=1006>
55. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис..д.ю.н. 12.00.07/ Т.Ю.Ткачук- Ужгород:Ужгородський національний університет.- 2019 - [Електронний ресурс].– Режим доступу: <https://www.uzhnu.edu.ua/uk/infocentre/get/19618>

## ДОДАТКИ

## Додаток А

Таблиця А.1.

## Global Cybersecurity Index 2018 [46]

| Member State   | Score | Regional Rank | Global Rank |
|----------------|-------|---------------|-------------|
| Israel*        | 0.783 | 24            | 39          |
| Portugal       | 0.758 | 25            | 42          |
| Monaco         | 0.751 | 26            | 43          |
| Latvia         | 0.748 | 27            | 44          |
| Slovakia       | 0.729 | 28            | 45          |
| Bulgaria*      | 0.721 | 29            | 46          |
| Slovenia*      | 0.701 | 30            | 48          |
| Moldova        | 0.662 | 31            | 53          |
| Ukraine        | 0.661 | 32            | 54          |
| Cyprus*        | 0.652 | 33            | 56          |
| Serbia         | 0.643 | 34            | 58          |
| Montenegro     | 0.639 | 35            | 61          |
| Albania        | 0.631 | 36            | 62          |
| Czech Republic | 0.569 | 37            | 71          |
| Romania        | 0.568 | 38            | 72          |
| Liechtenstein  | 0.543 | 39            | 75          |
| Greece         | 0.527 | 40            | 77          |





Рис. Б.1. Онлайн-ресурс «Security Tachometer»

Київський національний торговельно-економічний університет  
Кафедра публічного управління та адміністрування

**РЕФЕРАТ**  
**ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ**

на тему:

**МЕХАНІЗМ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ**  
**ВІД ЗОВНІШНІХ ВПЛИВІВ**

Студента 2-го курсу, 4-м групи,  
спеціальності 281 «Публічне  
управління та адміністрування»  
спеціалізації «Публічне  
управління та адміністрування»

Небога Ігор  
Владиславович

---

(підпис студента)

Науковий керівник  
к.е.н.  
доцент

Сонько  
Юлія  
Анатоліївна

---

(підпис керівника)

Гарант освітньої програми  
д-р. екон. наук,  
доцент

Ладонько  
Людмила  
Степанівна

---

(підпис гаранта)

Київ 2020

Випускна кваліфікаційна робота складається зі вступу, трьох розділів, висновків, 2 додатків, списку використаних джерел (55 найменувань). Основний зміст роботи викладено на 42 сторінках комп'ютерного тексту. Робота містить 9 рисунків, 1 таблицю.

Метою роботи є розроблення та обґрунтування організаційно-правових механізмів захисту інформаційного простору України від зовнішніх впливів.

Поставлена мета зумовила необхідність вирішення таких дослідницьких завдань:

- визначити сутність понять «інформаційний простір» та «інформаційна безпека»;
- визначити основні проблеми захисту інформаційного простору України;
- проаналізувати нормативно -правове забезпечення в інформаційній сфері;
- дослідити стан організаційно-правових механізмів державної політики в інформаційній сфері;
- визначити основні напрями державної інформаційної політики;
- проаналізувати механізми, що забезпечують ефективне функціонування інформаційних ресурсів;
- визначити основні загрози інформаційній безпеці України;
- розробити рекомендації щодо шляхів вдосконалення організаційно-правового забезпечення у сфері захисту інформаційного простору України.

Об'єктом дослідження є процес формування системи захисту інформаційного простору України.

Предметом дослідження є теоретико-методичні та прикладні основи механізмів захисту інформаційного простору України.

Для вирішення визначених завдань, у процесі дослідження використано загальнонаукові та спеціальні методи, зокрема: наукової абстракції – для розкриття понять «інформаційний простір» та «інформаційна безпека» та формування об'єкта дослідження; аналізу та синтезу – для виявлення необхідності створення ефективної системи захисту інформаційного простору; логічний метод – для формування шляхів вдосконалення організаційно-правових механізмів захисту інформаційного простору України від зовнішніх впливів.

У першому розділі розкриваються сутнісні характеристики інформаційного простору та інформаційної безпеки та визначається нормативно-правове забезпечення в інформаційній сфері.

У другому розділі здійснюється оцінювання стану організаційно-правових механізмів державної політики в інформаційній сфері та викладено пропозиції щодо удосконалення механізмів, що забезпечують ефективне функціонування інформаційних ресурсів.



У третьому розділі визначено основні загрози інформаційній безпеці України та розроблено конкретні рекомендації щодо вдосконалення організаційно-правових механізмів в інформаційній сфері.

Одержані результати можуть бути використані при удосконаленні роботи Міністерства культури та інформаційної політики.

### **Анотація**

У випускній кваліфікаційній роботі висвітлено основні проблеми захисту інформаційного простору України, проаналізовано основні напрями державної інформаційної політики, викладено пропозиції щодо удосконалення організаційно-правових механізмів захисту інформаційного простору України.

Ключові слова: інформаційний простір; інформаційна безпека; організаційно-правові механізми.

### **Annotation**

The final qualification project is concerned with main problems of defence of information space of Ukraine. It gives a detailed analysis of the state information policy direction. It is proposed ideas for improving organizational and legal mechanisms for the protection of the information space of Ukraine.

Key words: information space; informational security; organizational and legal mechanisms.

## РЕЦЕНЗІЯ

на випускну кваліфікаційну роботу

на тему: «**Механізм захисту інформаційного простору України від зовнішніх впливів**»,

студента ОС «Магістр»

спеціальності «Публічне управління та адміністрування»

Київського національного торговельно-економічного університету

**Небоги Ігоря Владиславовича**

Випускна кваліфікаційна робота виконана на актуальну тематику. Гарантування безпеки інформаційного простору держави є змістовною складовою її національної безпеки і вимагає впровадження системної державної політики у цій сфері, здатної забезпечити захист суспільства від негативних інформаційних впливів.

Важливим є визначення загроз інформаційній безпеці та основних проблем захисту інформаційного простору України. На даний момент головними загрозами для інформаційного суверенітету України є інформаційна війна з боку Росії, кіберзлочинність та недостатній рівень медіа-культури суспільства. До основних проблем захисту інформаційного простору в Україні можна віднести: негативні наслідки діяльності різних політичних сил, некомпетентність працівників державних установ та недосконалість технічного захисту інформаційного простору України.

На думку автора, необхідно розширювати методи протидії інформаційній війні та підвищувати інформаційну культуру громадян України, шляхов вдосконалення організаційно-правових механізмів захисту інформаційного простору. Автор пропонує розробити систему заходів, яка включатиме створення Адженди інформаційної політики України, імплементацію у нормативно-правове поле України поняття «інформаційна агресія» та розробку інструментарію для регулювання питань інформаційної агресії, а також інші заходи з боку держави, спрямовані на захист інформаційного суверенітету України.

Випускна кваліфікаційна робота є актуальною та містить практичні рекомендації. Робота відповідає основним вимогам та може бути допущеною до захисту.

Голова громадської організації  
«Територіальні ініціативи»

Шляхтіна І.В.





Завідувачу кафедри публічного  
управління та адміністрування  
Новіковій Н.Л.

### Заява

Я, Небога Ігор Владиславович, повідомляю, що за результатами здійснення самостійної перевірки з використанням програмно-технічних засобів у наданій випускній кваліфікаційній роботі на тему: «Механізм захисту інформаційного простору України від зовнішніх впливів» не міститься елементів академічного плагіату. У випадках використання прямих запозичень з друкованих та електронних джерел, вказані відповідні посилання.

Робота для перевірки надається у друкованому та електронному варіантах. Електронна версія роботи ідентична з друкованою.

«14» 11 2020 року

 (підпис)



### Згода

Я, Небога Ігор Владиславович, цим засвідчую, що є автором випускної кваліфікаційної роботи на тему: «Механізм захисту інформаційного простору України від зовнішніх впливів» несу повну відповідальність за достовірність, точність та повноту поданої у роботі інформації, жодна частина роботи не була скопійована, за винятком випадків, коли робиться належне підтвердження в присвоєнні. Я підтверджую, що у роботі не міститься державної таємниці або інформації для службового користування.

Цим засвідчую, що жодна частина цієї роботи не була опублікована мною раніше.

Я даю дозвіл на те, що моя робота буде направлена в інституційний депозитарій Київського національного торговельно-економічного університету і збережена в базі даних для майбутньої перевірки плагіату.

28. 11 2020 року

Небога І.В.



# Кабинет<sup>?</sup>



ДОБАВИТЬ ДОКУМЕНТ



ДОБАВИТЬ ТЕКСТ



Поиск по названиям документов



1/2



ПЕРЕПРОВЕРИТЬ



ПЕРЕМЕСТИТЬ



УДАЛИТЬ



ИСТОРИЯ ОТЧЕТОВ



Название



Дата загрузки



Оригинальность



Небога\_Диплом



22 Ноя 2020  
23:08

86,56%

ПОСМОТРЕТЬ РЕЗУЛЬТАТЫ

[Главная](#) / [Инструменты](#) / Проверка уникальности текста

Актуальність теми: В умовах розвитку інформаційного суспільства та широкосмугового доступу до мережі Інтернет зростає значення інформаційного захисту та інформаційної безпеки держави. Необхідність гарантування інформаційної безпеки як змістовної складової національної безпеки зумовлюється існуванням загроз для інформаційної сфери країни, що можуть спричинити негативний вплив на свідомість населення України.  
У сучасних умовах конфлікту на Сході України дослідження питань, пов'язаних з безпекою

[← Проверить другой текст](#)

Унікальність 89%

<http://academy.gov.ua/ej/ej...>  
Совпадение: 3%

[Главная](#) / [Инструменты](#) / Проверка уникальности текста

Зміцнення та захист національного інформаційного простору України є складовою частиною забезпечення її національної безпеки. У сучасних реаліях військовий конфлікт на Сході України доводить те, що завоювання частини територій призвело до втрати контролю над інформаційним полем України і загрожує масовим розповсюдження інформаційного на культурного продукту супротивника.

[← Проверить другой текст](#)

Унікальність 84%

<http://dspace.nbuv.gov.ua/b...>  
Совпадение: 5%



[Главная](#) / [Инструменты](#) / Проверка уникальности текста

На думку І. Громико, Т. Саханчук, інформаційна безпека – це стан захищеності державних інтересів, який досягається шляхом моніторингу, виявлення і знищення, як внутрішніх, так і зовнішніх інформаційних загроз, та забезпечення міжнародного співробітництва у цій сфері[8]. Інформаційна безпека держави є важливим елементом усіх сфер національної безпеки країни. В той же час інформаційна безпека – це окрема та незамінна галузь забезпечення національної

[← Проверить другой текст](#)

Унікальність 88%

[https://mkip.gov.ua/done\\_i...](https://mkip.gov.ua/done_i...)

Совпадение: 4%

[Главная](#) / [Инструменты](#) / Проверка уникальности текста

У своїй діяльності Міністерство інформаційної політики України базувалося виключно на принципах захисту свободи слова та думки, захисту прав громадян на вираження своєї позиції. При МІП створено Громадську раду, до якої входили представники громадських організацій та засобів масової інформації, науковці. Вона виконувала функції нагляду за діяльністю Міністерства та надавала поради щодо напрямів розвитку країни з впровадженням

[← Проверить другой текст](#)

Унікальність 88%

<http://idpnan.org.ua/files/de...>

Совпадение: 2%

Діяльність журналістів в Україні регулюється Законом України «Про державну підтримку засобів масової інформації та соціальний захист журналістів», який гарантує права пільги та компенсацію за роботу із шкідливими та важкими умовами праці, охорону праці журналістів, на медичні огляди, соціальне страхування, на повне розслідування нещасних випадків, смерті і шкоди, яка була завдання здоров'ю журналіста при виконанні службових обов'язків. Згідно цього закону службова діяльність журналіста не може бути підставою для його затримання, арешту, а також вилучення опрацьованих, зібраних, підготовлених ним матеріалів та технічних засобів, які він використовує для виконання своєї роботи[23].

← Проверить другой текст

Унікальність 88%

<http://www.pravoznavec.co...>

Совпадение: 5%

<https://www.radiosvoboda.o...>

Совпадение: 3%

PR·CY



Тарифы и цены

Инструменты

Биржа сайтов

Q&A

Блог

Улучшить аккаунт



Главная / Инструменты / Проверка уникальности текста

В. Гусаров, досліджуючи проблему інформаційної безпеки України, стверджує, що Росія здійснює інформаційно-психологічні атаки, щоб активізувати поширення конфлікту на сході України, здійснювати тиск на українське управління, щоб змусити його погодитись на російський сценарій урегулювання конфлікту. В. Гусаров виокремлює такі напрями інформаційно-психологічних атак проти України[25].

← Проверить другой текст

Унікальність 88%

<http://www.molodyvcheny.in...>

Совпадение: 5%

Активация Windows

Чтобы активировать Windows, перейдите в меню «Параметры».

[Главная](#) / [Инструменты](#) / Проверка уникальности текста

У даному положенні термін «система електронної взаємодії державних електронних інформаційних ресурсів» тлумачиться як система призначена для автоматизації та технологічного забезпечення обміну електронними даними між суб'єктами владних повноважень з державних електронних інформаційних ресурсів під час надання адміністративних послуг та здійснення інших повноважень відповідно до покладених на них завдань шляхом використання відповідних сервісів, що є інтерфейсами прикладного програмування доступу до державних електронних інформаційних ресурсів, створеними згідно з єдиними вимогами, а також шляхом використання єдиних протоколів, форматів, шаблонів довідників та класификаторів [31]

[← Проверить другой текст](#)

Уникальность 83%

<https://dostup.pravda.com.ua/>  
Соподобление: 5%<https://zakon.rada.gov.ua/g>  
Соподобление: 5%<https://zakon.rada.gov.ua/g>[Главная](#) / [Инструменты](#) / Проверка уникальности текста

Особливої уваги вимагає законодавство про засоби масової інформації, законодавство про формування інформаційних ресурсів, законодавство про інформаційну та кібернетичну безпеку, законодавство про порядок реалізації права на пошук, отримання, передачу та використання інформації, а також необхідним є створення широкого спектру інформаційних продуктів, надання інформаційних послуг[51]

[← Проверить другой текст](#)

Уникальность 95%

<http://ea.donntu.edu.ua/bits/>  
Соподобление: 2%

Актив  
Чтобы ак  
раздел "