МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІМ. Ю.М. ПОТЕБНІ

Кафедра управління та адміністрування

Кваліфікаційна робота(проєкт)

магістр
(рівень вищої освіти)

НА ТЕМУ: УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ

Виконав: студент другого курсу, групи 8.2812-2з
Спеціальності 281 «Публічне управління та адміністрування»
(код і назва спеціальності)

освітньої програми Публічне управління та адміністрування
(назва освітньої програми)
Івасів Юрій Борисович
(ініціали та прізвище)

Керівник: Фурсін О.О., доцент кафедри управління та адміністрування, кандидат наук з державного управління
(посада, вчене звання, науковий ступінь, прізвище та ініціали)
Рецензент Воронкова В.Г., зав.кафедри управління та адміністрування, професор, доктор філософських наук
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя
2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Інженерний навчально-науковий інститут ім. Ю.М. Потебні
Кафедра управління та адміністрування
Рівень вищої освіти магістр
Спеціальність 281 «Публічне управління та адміністрування»
(код та назва)
Освітня програма Публічне управління та адміністрування

ЗАТВЕРДЖУЮ
Завідувач кафедри д.філос.н.,
проф.Воронкова В.Г. _____
«___» _____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ) СТУДЕНТОВІ (СТУДЕНТЦІ)

Івасів Юрій Борисович
(прізвище, ім'я, по батькові)

1. Тема роботи (проєкту) *Удосконалення інформаційної політики органів публічного управління*
керівник роботи *Фурсін О.О., доцент кафедри управління та адміністрування, кандидат наук з державного управління*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ЗНУ від «01» 09.2023 року № 636-С
2.Строк подання студентом роботи 01 грудня 2023 р.
3.Вихідні дані до роботи 1. Формування плану. 2. Формування гіпотези дослідження. 3. Аналіз літературних джерел за останні п'ять років. 5. Методологія дослідження.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *1. Теоретико-методологічні засади інформаційної політики органів публічного управління. 2. Аналітико-дослідницькі виміри напрямів удосконалення інформаційної політики органів публічного управління*
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	Фурсін О.О., доцент кафедри управління та адміністрування, кандидат наук з державного управління	01.10.23	
Розділ 2	Фурсін О.О., доцент кафедри управління та адміністрування, кандидат наук з державного управління	01.12.23	
Нормоконтроль	Венгер О.М., к.п.н., доц. кафедри управління та адміністрування		

7. Дата видачі завдання 30 червня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	З'ясувати теоретичні засади інформаційної політики органів публічного управління	15.09.23	
2	Сформувати понятійно-категоріальний інформаційної політики органів публічного управління	01.10.23	
3	Розкрити методи та засоби удосконалення інформаційної політики органів публічного управління	15.10. 23	
4	Виявити діагностику проблем інформаційної політики органів публічного управління	30.10.23	
5	Дослідити напрями удосконалення інформаційної політики органів публічного управління	17.11.23	
6	Запропонувати інструменти удосконалення інформаційної політики органів публічного управління	25.11.23	
7	Обґрунтувати складові інформаційної політики органів публічного управління	30.11.23	
8	Розробити практичні рекомендації щодо удосконалення інформаційної політики органів публічного управління	02.12.23	

Студент _____ Івасів Ю.Б.
(підпис) (ініціали та прізвище)

Керівник роботи (проєкту) _____ О.О.Фурсін
(підпис) (ініціали та прізвище)

Нормоконтроль пройдено
Нормоконтролер _____ О.М.Венгер
(підпис) (ініціали та прізвище)

АНОТАЦІЯ

Івасів Ю.Б. Удосконалення інформаційної політики органів публічного управління.

Кваліфікаційна робота для здобуття ступеня вищої освіти магістра за спеціальністю 281 «Публічне управління та адміністрування», науковий керівник О.О. Фурсін. Запорізький національний університет. Інженерний навчально-науковий інститут ім. Ю.М.Потебні. Кафедра управління та адміністрування, 2023.

В кваліфікаційній роботі розглянуто теоретико-методологічні засади інформаційної політики органів публічного управління. Розглянуто особливості напрямів удосконалення інформаційної політики органів публічного управління. Певна увага приділяється виявленню перспектив і недоліків напрямів удосконалення інформаційної політики органів публічного управління для для забезпечення ефективності та прозорості державного апарату.

Ключові слова: ІНФОРМАЦІЙНА ПОЛІТИКА, ЦИФРОВА ТРАНСФОРМАЦІЯ, КІБЕРБЕЗПЕКА, ВІДКРИТІ ДАНІ, ЕЛЕКТРОННЕ УПРАВЛІННЯ ДОКУМЕНТАМИ, СТАНДАРТИЗАЦІЯ ДАНИХ

ABSTRACT

Ivasiv Yu. Improving the information policy of public administration agencies.

Qualifying work for obtaining a master's degree in higher education, specialty 281 «Public management and administration», supervisor O. Fursin. Zaporizhzhia National University. Engineering Educational and Scientific Institute named after Y. Potebny. Department of management and administration, 2023.

The theoretical and methodological principles of the information policy of public administration bodies are considered in the qualification work. The peculiarities of directions for improving the information policy of public administration bodies are considered. A certain amount of attention is paid to the identification of prospects and shortcomings of areas for improving the information policy of public administration bodies to ensure the efficiency and transparency of the state apparatus.

Keywords: INFORMATION POLICY, DIGITAL TRANSFORMATION, CYBER SECURITY, OPEN DATA, ELECTRONIC DOCUMENT MANAGEMENT, DATA STANDARDIZATION

ЗМІСТ

ВСТУП

Реалізація інформаційної політики органів публічного управління має базуватися на комплексі правових механізмів та організаційних заходів для досягнення позитивних ефектів: узгодження інтересів людини, суспільства та країни в інформаційному просторі; запобігання незаконному розповсюдженню, використанню та порушенню цілісності інформації. Сучасний стан українського суспільного розвитку та світового інформаційного простору вимагає посилення ролі держави у забезпеченні доступу громадян України до ефективної та об'єктивної інформації та забезпеченні захисту національного інформаційного простору від негативної інформації [1]. У зв'язку з цим актуальним стає розробка відповідної національної інформаційної політики для протистояння зовнішнім загрозам. Питання переліку пріоритетних напрямків інформаційної політики органів публічного управління потребує особливої уваги, оскільки їх раціональний та науково обґрунтований вибір зосередить зусилля науковців, державних службовців та посадових осіб відповідних національних органів влади та інститутів громадянського суспільства на формування пріоритетних напрямів суспільного життя та виконання комплексу завдань, спрямованих на реалізацію основних положень державної інформаційної політики.

Дослідженню напрямків державної інформаційної політики України присвячено праці багатьох українських дослідників, таких як І.Арістова, В.Воронкова, І.Волков, О.Гіда, О. Голобуцький, Г. Головко, В. Дзюндзюк, Н.Заниздра, С. Зуєв, Ю.Іванченко, Н. Корніловська, Г.Красноступ, О. Крюков, З Кузнецова, Ю.Максименко, Л.Мамчур, Ю. Машкаров, О. Марченко, Д. Мельник, Н.Медведєва, О.Мостовенко, О.Олійник, О. Орлов, М.Пахнін, В.Негодченко, Ю.Нестеряк, Н.Новицька, ВСавченко, В.Стєклов, В.Степанов, О.Соснін, О.Орлов, Л.Терещенко, О.Токар, В. Тронь, А.Черемнова,О. Шевчук, О Шишка,С. Чукут та інші.

Предметом дослідження є теоретичне обґрунтування удосконалення інформаційної політики органів публічного управління.

Об’єктом дослідження є процес формування інформаційної політики органів публічного управління.

Метою роботи є вивчення теоретичних основ формування та реалізації напрямів удосконалення інформаційної політики органів публічного управління.

Для досягнення поставленої мети були визначені такі основні завдання:

– визначити принципи, завдання та методи інформаційної політики органів публічного управління;

– розглянути проблеми, що виникають в управлінні інформаційної політики органів публічного управління;

– проаналізувати світовий інформаційної політики органів публічного управління;

– провести аналіз системи управління інформаційної політики органів публічного управління а;

– провести діагностування інформаційної політики органів публічного управління;

– навести основні напрямки удосконалення інформаційної політики органів публічного управління;

– надати пропозиції щодо впровадження інформаційної політики органів публічного управління.

У процесі дослідження використано такі загальнонаукові методи і прийоми, як: монографічний – для детального вивчення теоретико-методичних засад інформаційної політики органів публічного управління; аналізу і синтезу, індукції та дедукції – для постановки проблеми дослідження, вивчення і деталізації об’єкта дослідження; статистичного та техніко-економічного аналізу – для узагальнення факторів і показників інформаційної політики органів публічного управління; експертних оцінок й аналізу ієрархій – для оцінки стратегічних досліджень інформаційної

політики органів публічного управління; системного аналізу – для вивчення організаційно-методичних засад моніторингу потенціалу інформаційної політики; графічний – для наочного та схематичного зображення теоретичних і практичних результатів дослідження; факторного аналізу – для оцінки ефективності управління інформаційної політики органів публічного управління.

Інформаційною базою дослідження є фундаментальні положення сучасної економічної теорії, державного управління, результати наукових досліджень вітчизняних і зарубіжних вчених, закони України, постанови, рішення уряду з найважливіших питань регулювання інформаційної політики органів публічного управління, дані офіційної статистики, а також первинні матеріали, зібрані автором особисто.

Наукова новизна одержаних результатів полягає в розробці практичних рекомендацій щодо удосконалення інформаційної політики органів публічного управління.

Практичне значення отриманих результатів полягає у наданні конкретних рекомендацій, що створюють вагоме підґрунтя для формування інформаційної політики органів публічного управління.

Матеріали робіт та результати досліджень схвалюються на всеукраїнських науково-практичних конференціях, зокрема в міжнародній науково-практичній конференції «Формування цифрових компетентностей у процесі викладання дисциплін «цифрової гуманітаристики» та управлінсько-економічного циклу в умовах діджиталізації» 22-23 листопада 2023 року.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ

1.1. Методологія дослідження інформаційної політики органів публічного управління

Методологія дослідження інформаційної політики органів публічного управління може бути створена на основі ряду підходів та методів, щоб забезпечити систематичний та обґрунтований аналіз. Нижче наведено загальний методологічний підхід для дослідження інформаційної політики:

1. Визначення об'єкта дослідження (інформаційна політика органів публічного управління) та суб'єктів (органи влади, відповідальні за формування та виконання інформаційної політики).

2. Поглиблене вивчення теоретичних засад інформаційної політики, враховуючи концепції, моделі та методології в галузі інформаційної безпеки та управління даними.

3. Формулювання конкретної мети дослідження та визначення основних завдань, які слід вирішити для досягнення цієї мети.

4. Вибір підходів та методів дослідження, таких як аналіз документів, експертні опитування, вивчення випадків, опитування співробітників та аналіз статистичних даних.

5. Розробка анкет, інтерв'ю та інших інструментів для збору необхідної інформації.

6. Здійснення збору даних з використанням розроблених інструментів та їх аналіз з використанням статистичних методів чи кількісних та якісних підходів.

7. Інтерпретація результатів дослідження та формулювання висновків,

які відповідають на запитання дослідження та визначають його значущість.

8. На основі отриманих результатів розробка рекомендацій для вдосконалення інформаційної політики органів публічного управління.

9. Підготовка наукового звіту та можливої публікації результатів дослідження.

Методологія надає структурований підхід до дослідження інформаційної політики органів публічного управління та може бути адаптована залежно від конкретного контексту та обставин дослідження.

Системний підхід дослідження інформаційної політики органів публічного управління орієнтується на розуміння організації як системи, що включає в себе взаємопов'язані елементи та процеси. Дослідження здійснюється з урахуванням цілісності, взаємодії та впливу різних аспектів інформаційної політики на функціонування органів публічного управління. Розглянемо етапи системного підходу до дослідження інформаційної політики:

– ідентифікація системних елементів, що входять до складу інформаційної політики: стратегії, процедури, технології, організаційні структури, персонал тощо;

– аналіз взаємодії між різними елементами інформаційної політики, вплив одного елемента на інший та визначення ключових взаємодій;

– оцінка ефективності інформаційної політики: досягнення стратегічних цілей, якість обробки інформації, рівень безпеки, доступність та інші аспекти;

– ідентифікація залежностей між інформаційною політикою та іншими аспектами управління, такими як кадри, фінанси, стратегії тощо;

– розробка системної моделі, що відображає систему інформаційної політики, включаючи всі ідентифіковані елементи та їх взаємозв'язки;

– синтез та висновки: спроба зрозуміти систему в цілому, враховуючи усі складові та їх взаємодії; формулювання висновків та синтез інформації для розуміння сутності інформаційної політики;

– на основі виявлених взаємозв'язків та слабких місць системи розробляються рекомендації щодо вдосконалення інформаційної політики;

– здійснення впровадження запропонованих рекомендацій з метою покращення інформаційної політики.

Системний підхід дозволяє розглядати інформаційну політику як складну систему з взаємозалежними елементами, що дозволяє глибше розуміти її функціонування та виявляти можливості для оптимізації.

Системно-структурний підхід дослідження інформаційної політики органів публічного управління базується на концепції, що організація та її інформаційна політика розглядаються як складові частини більшої системи; всі елементи та підсистеми взаємодіють між собою та утворюють велику інтегровану систему. Основні принципи системно-структурного підходу в дослідженні інформаційної політики включають:

–розгляд інформаційної політики як системи, яка складається з взаємопов'язаних елементів та підсистем (організаційна структура, процеси, технології, людські ресурси та інші аспекти);

–визначення взаємозв'язків та взаємодії між елементами системи (наприклад, як впливає інформаційна політика на процеси прийняття рішень, на комунікацію в організації, на відносини з громадськістю та інші аспекти);

–розгляд структури інформаційної політики, включаючи розподіл влади та обов'язків, організаційні процеси, ресурси та інші елементи;

–визначення основних функцій та завдань, які виконує інформаційна політика, а також їх вплив на досягнення стратегічних цілей організації.

–вивчення системи звітності та контролю в контексті інформаційної політики, визначення механізмів відстеження та оцінки результативності політичних заходів;

–врахування змін та розвитку системи інформаційної політики в часі; Розгляд інформаційної політики як динамічної системи, яка адаптується до змін у внутрішньому та зовнішньому середовищі;

Системно-структурний підхід дозволяє отримати глибоке розуміння

системної природи інформаційної політики, враховуючи комплексні взаємодії та взаємозв’язки між всіма її елементами.

Аксіологічний підхід до дослідження інформаційної політики органів публічного управління зосереджений на вивченні цінностей, переконань, ідеологій та етичних аспектів, які впливають на формування та реалізацію інформаційних стратегій та політик. Проаналізуємо основні аспекти аксіологічного підходу дослідження інформаційної політики: визначення основних цінностей, які лежать в основі інформаційної політики (прозорість, відкритість, демократію, ефективність, інновації тощо); аналіз етичних аспектів інформаційної політики, враховуючи питання конфіденційності, правдивості інформації, захисту приватності та інші етичні засади; врахування впливу соціокультурного середовища на формування цінностей, які визначають інформаційну політику; оцінка того, наскільки інформаційна політика відповідає загальноприйнятим цінностям та чи має вона суспільну підтримку; аналіз взаємозв'язку між цінностями та відповідальністю в інформаційній діяльності (питання відповідального використання інформації, захисту прав громадян та інші етичні аспекти); розгляд питань, пов'язаних із забезпеченням легітимності інформаційної політики для підвищення довіри громадськості.

Аксіологічний підхід дозволяє розглядати інформаційну політику як частину соціокультурного контексту та враховувати цінності, які лежать в основі рішень і стратегій управління інформацією в сфері публічного управління.

Компаративний підхід дослідження інформаційної політики органів публічного управління передбачає порівняння та аналіз інформаційних стратегій, політик і практик різних країн чи органів з метою виявлення схожих або відмінних рис, успіхів та недоліків. Цей підхід дозволяє зрозуміти, які фактори впливають на ефективність інформаційної політики та як краще використовувати ці знання для покращення власної практики. Основні етапи компаративного підходу дослідження інформаційної

політики:

1) визначення країн, регіонів або органів публічного управління, які будуть об'єктом порівняння;

2) визначення конкретних питань або аспектів інформаційної політики, які будуть порівнюватися;

3) збір інформації про стратегії, правові акти, технологічні рішення та інші аспекти інформаційної політики в обраних об'єктах дослідження;

4) використання аналітичних методів для порівняння зібраних даних та ідентифікації спільних або відмінних рис;

5) аналіз та інтерпретація виявлених різниць чи подібностей, а також їх можливих причин;

6) визначення ключових висновків та розробка рекомендацій на основі проведеного порівняльного аналізу.

Компаративний підхід дозволяє враховувати контекст та специфіку різних систем управління та інформаційної політики. Такий аналіз може бути корисним для установ та країн, оскільки він надає можливість враховувати найкращі практики та уникати помилок, адаптуючи чи застосовуючи досвід інших.

Синергетичний підхід до дослідження інформаційної політики органів публічного управління базується на концепціях синергетики, яка вивчає взаємодію та виникнення нових структур та властивостей в системах. В контексті дослідження інформаційної політики, синергетичний підхід розглядає інформаційну політику як динамічну систему, що може розвиватися, адаптуватися та взаємодіяти з навколишнім середовищем. Ось деякі ключові аспекти синергетичного підходу:

–дослідження інформаційної політики з урахуванням неоднорідності та взаємодії різних компонентів. врахування того, що різні елементи інформаційної політики можуть мати відмінні характеристики та впливати один на одного;

–розгляд інформаційної політики як системи, яка може змінюватися та

адаптуватися до змін у своєму оточенні. вивчення динаміки змін в інформаційній політиці з часом;

–вивчення емерджентних властивостей та структур у системі інформаційної політики, які можуть виникнути в результаті взаємодії компонентів;

–розгляд нелінійних взаємодій між різними елементами інформаційної політики, де невеликі зміни можуть мати значущий вплив на систему в цілому;

–розгляд системи як здатної до самоорганізації та самовідновлення, здатної адаптуватися до змін та виправляти неполадки;

–вивчення інформаційної політики з урахуванням контексту органів публічного управління та його впливу на формування та реалізацію політики;

–звернення уваги на граничні умови та точки взаємодії, які можуть призводити до критичних змін в системі.

Синергетичний підхід дозволяє досліджувати інформаційну політику як живий та динамічний процес, враховуючи взаємодію різних факторів та властивостей. Цей підхід може допомогти краще зрозуміти природу інформаційної політики та розробити більш гнучкі стратегії управління інформацією в органах публічного управління.

Функціональний підхід дослідження інформаційної політики органів публічного управління базується на розгляді цієї політики як системи функцій, що виконуються для досягнення стратегічних цілей та завдань. В рамках цього підходу, інформаційна політика розглядається як сукупність функцій та завдань, спрямованих на забезпечення ефективного управління інформацією в органах публічного управління. Зазначимо декілька ключових аспектів функціонального підходу:

1. Ідентифікація основних функцій, які виконує інформаційна політика в органах публічного управління, що включає функції забезпечення безпеки інформації, збору та аналізу даних, забезпечення доступності та інші.

2. Вивчення та аналіз конкретних функціональних обов'язків, які

покладені на інформаційну політику (управління документацією, ведення баз даних, впровадження технологій тощо).

3. Вимірювання ефективності виконання різних функцій інформаційною політикою (оцінка досягнення стратегічних цілей та міркувань ефективності використання ресурсів).

4. Розгляд інформаційної політики як інтегрованої системи функцій, що взаємодіють для забезпечення цілісності та ефективності управління інформацією.

5. Визначення та аналіз можливостей адаптації інформаційної політики до змін внутрішнього та зовнішнього середовища.

6. Вдосконалення функціональних процесів інформаційної політики для забезпечення оптимальної ефективності та ефективності.

7. Вивчення взаємодії інформаційної політики з іншими системами в органах публічного управління, такими як управління персоналом, фінансові системи тощо.

Функціональний підхід дозволяє досліджувати інформаційну політику як набір конкретних функцій та процесів, які виконуються для досягнення стратегічних цілей органів публічного управління. Врахування цих аспектів дозволяє зрозуміти, як ефективно використовується інформація в управлінні та як можна поліпшити виконання різних функцій.

Структурно-функціональний підхід дослідження інформаційної політики органів публічного управління базується на вивченні взаємозв'язків між структурними елементами системи та їхніми функціями. Цей підхід дозволяє розглядати органи публічного управління як систему, де різні структурні компоненти виконують певні функції для досягнення стратегічних цілей. Основні аспекти структурно-функціонального підходу дослідження інформаційної політики: визначення структурних компонентів організації, таких як підрозділи, відділи, комітети та інші структурні одиниці; аналіз функцій, які виконують різні структурні компоненти органів публічного управління у сфері інформаційної політики; вивчення взаємодії

та комунікацій між різними структурними одиницями, що забезпечують реалізацію інформаційної політики; визначення, як розподіляється влада та відповідальність між різними рівнями та структурними одиницями органів публічного управління; вивчення функціональних процесів, які спрямовані на забезпечення інформаційної безпеки, обробку даних, комунікації тощо; аналіз того, як органи публічного управління взаємодіють з зовнішніми агентами, включаючи громадськість, бізнес.

Цей підхід дозволяє досліджувати інформаційну політику як систему, в якій структурні компоненти виконують свої функції для забезпечення ефективної реалізації стратегій та досягнення цілей. Враховуючи структурно-функціональні взаємозв'язки, можна отримати глибше розуміння того, як діє інформаційна політика в органах публічного управління.

Аналітичний підхід дослідження інформаційної політики органів публічного управління передбачає використання методів та інструментів аналізу для збору, обробки та висвітлення інформації. Цей підхід спрямований на розкриття ключових питань, виявлення тенденцій та розуміння проблем у сфері інформаційної політики. Розглянемо етапи аналітичного підходу:

1. Визначення конкретних дослідницьких питань, на які дослідження інформаційної політики повинно відповісти (питання можуть стосуватися ефективності, безпеки, доступності інформації тощо).

2. Визначення методів аналізу, які будуть використані для опрацювання даних (статистичний аналіз, SWOT-аналіз, контент-аналіз, вивчення випадків, експертні опитування тощо).

3. Здійснення збору необхідних даних для дослідження (аналіз документів, статистичних даних, проведення опитувань та інших джерел).

4. Використання статистичних методів для опису, аналізу та інтерпретації (визначення середніх значень, варіаційний аналіз, кореляційний аналіз тощо).

5. SWOT-аналіз: аналіз сильних та слабких сторін, можливостей та

загроз, пов'язаних з інформаційною політикою, що допомагає визначити внутрішні та зовнішні фактори, що впливають на політику.

6. Залучення експертів для отримання кваліфікованої оцінки конкретних аспектів інформаційної політики.

7. Контент-аналіз текстової інформації для виявлення ключових тем, термінів та зв'язків.

8. Детальний аналіз конкретних випадків або ситуацій для розуміння конкретних аспектів інформаційної політики.

9. Формулювання висновків на основі проведеного аналізу та розробка рекомендацій для поліпшення інформаційної політики.

10. Використання візуалізаційних засобів (графіки, діаграми) для чіткого представлення результатів та сприяння легшому їх розумінню.

Аналітичний підхід дозволяє глибоко досліджувати інформаційну політику, використовуючи систематичні методи аналізу для отримання обґрунтованих та об'єктивних результатів.

Неоінституційний підхід дослідження інформаційної політики органів публічного управління базується на розгляді впливу інституціональних факторів, таких як норми, правила, процедури, традиції та соціокультурний контекст, на формування та реалізацію інформаційних стратегій та політик в органах управління. Основні риси неоінституційного підходу включають:

Акцент на ролі інститутів, тобто усталених правил гри, у формуванні та реалізації інформаційної політики (формальні правові норми, і неформальні правила, традиції та інші норми); дослідження впливу соціокультурних норм і звичаїв на формування підходів до обробки, збереження та передачі інформації; розгляд інформаційної інфраструктури як важливого елемента інституціонального середовища, який визначає можливості та обмеження інформаційної політики; розгляд реакції інформаційної політики на зміни в інституціональному середовищі, а також вивчення процесів адаптації та еволюції; аналіз владних відносин у контексті інформаційної політики, включаючи питання розподілу влади та впливу

різних акторів; вивчення того, як позитивні або негативні інституційні впливи можуть сприяти або стримувати розвиток інформаційної політики.

Неоінституційний підхід дозволяє зосередитися на контексті та умовах, які визначають формування та реалізацію інформаційної політики в органах публічного управління, враховуючи різноманітні аспекти інституціонального середовища.

Таким чином, методологія дослідження інформаційної політики органів публічного управління визначає рамки, принципи та підходи, які використовуються для проведення дослідження з даної області.

1.2. Теоретичні засади інформаційної політики органів публічного управління

Вважаємо за необхідне проаналізувати основні аспекти інформаційної політики органів публічного управління через сукупність конкретних концептуальних уявлень, які взаємоузгоджені та утверджені з урахуванням інтересів і потреб громадян, суспільства та держави в певних сферах життя. Необхідно дослідити об'єкти, суб'єкти, цілі та засоби політики [23].

Усі громадяни, юридичні особи та державні установи України мають право на інформацію, що дає їм можливість вільно отримувати, використовувати, поширювати і зберігати інформацію, необхідну для здійснення своїх прав, свобод і законних інтересів, а також виконання покладених на них завдань. і функції. Громадяни, юридичні особи і держава реалізують своє право знати і не завдавати шкоди громадським, політичним, економічним, соціальним, духовним, екологічним та іншим правам, свободам і законним інтересам інших громадян, а також правам та інтересам юридичних осіб. Кожен громадянин має вільний доступ до інформації, що його стосується, крім випадків, передбачених законодавством України.

Інформаційна політика органів публічного управління – це вплив держави на розвиток сфери соціальної інформації, зокрема телекомунікацій, інформаційних систем, засобів масової інформації та діяльність, пов’язану з реєстрацією, пошуком, отриманням, створенням, обробкою, використанням, зберіганням, розповсюдженням, відображенням та пов’язаною з ними діяльність щодо передачі різних видів інформації.

Об'єктом інформаційної політики є інформація як важливий ресурс, який використовується органами публічного управління для досягнення своїх цілей і завдань, що має різноманітні типи інформації, такі як:

1. Конфіденційна інформація – це матеріали, які є обмеженими в доступі та не призначені для загального розголошення. Ця інформація може містити персональні дані, які потребують особливого захисту з міркувань безпеки, конфіденційності та законності.

У Законі України «Про доступ до публічної інформації» «конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов» [24]

В табл. 1.1 представлено основні характеристики конфіденційної інформації в органах публічного управління.

Таблиця 1.1 – Основні характеристики конфіденційної інформації в органах публічного управління

Особиста інформація громадян	Персональні дані: інформація, пов'язана з особистістю громадян, така як імена, адреси, номери телефонів, ідентифікаційні номери тощо. Медична інформація: інформація про стан здоров'я громадян, яка вимагає особливого захисту.
Комерційна інформація	Договори та угоди: конфіденційні деталі комерційних угод та договорів, які укладаються органами публічного управління.

	Фінансова інформація: конфіденційні фінансові дані, включаючи бюджети, витрати, фінансові плани тощо.
Стратегічна інформація	Плани та стратегії: конфіденційні плани та стратегії, спрямовані на досягнення стратегічних цілей органу управління. Службові та політичні стратегії: конфіденційна інформація, пов'язана з внутрішніми процесами та політичними рішеннями.
Інформація з питань безпеки	Плани екстреного реагування: конфіденційна інформація, яка стосується планів та заходів у випадку екстрених ситуацій. Інформація з безпеки нації: конфіденційні дані, пов'язані з національною безпекою та оборонною стратегією.
Службові та внутрішні документи	Внутрішні директиви та інструкції: конфіденційні документи, які регулюють внутрішню діяльність та процеси управління.
Інформація, що стосується розслідувань та правопорушень	Результати розслідувань: конфіденційна інформація про розслідування правопорушень та інші службові розслідування.

Органи публічного управління відповідають за захист конфіденційної інформації та використання її в межах Закону України «Про захист персональних даних», Закону України «Про інформацію» та нормативів, а також за забезпечення доступності цієї інформації лише тим особам, які мають на це право.

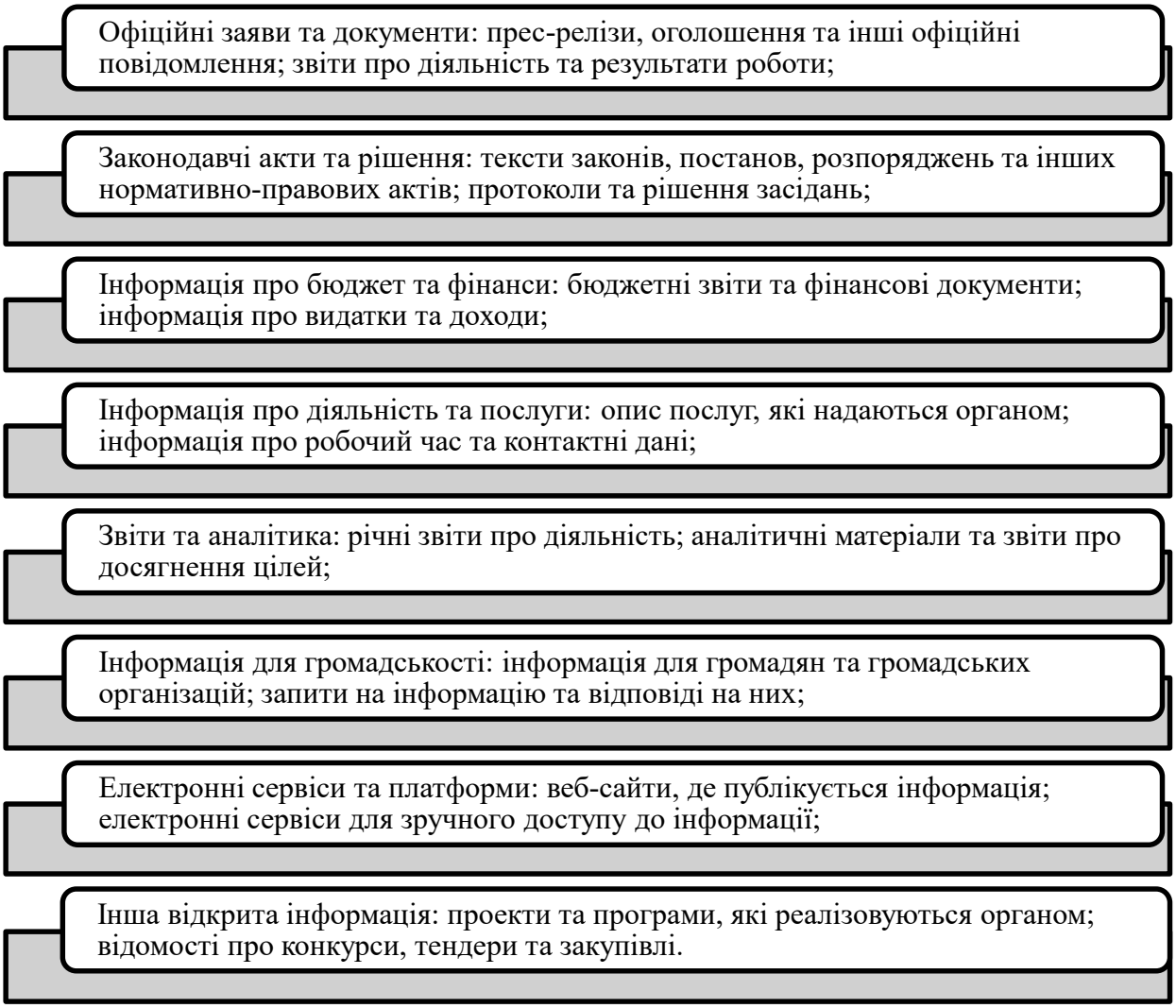
2. Публічна інформація органів публічного управління – це інформація, яка є відкритою для загального доступу та призначена для інформування громадськості та інших зацікавлених сторін.

Згідно Закону України «Про доступ до публічної інформації», «публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом». Метою цього Закону є забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації [24.

Органи публічного управління мають відповідальність забезпечувати прозорість та доступність певної частини своєї інформації відповідно до

законодавства (рис. 1.1).

Рисунок 1.1. Види публічної інформації органів публічного управління



Важливо зауважити, що доступ до публічної інформації регулюється Законом України «Про доступ до публічної інформації» та місцевими нормативами. Забезпечення доступності та якості публічної інформації є важливим аспектом взаємодії органів публічного управління і громадян.

3. Стратегічна інформація органів публічного управління – це особливий вид інформації, яка визначає стратегічні цілі, завдання, напрямки та плани діяльності організації в середньо- та довгостроковій перспективі. Ця інформація включає ключові аспекти, спрямовані на досягнення місій та стратегічних цілей органу публічного управління. Вона може бути класифікована як конфіденційна та публічна інформація з обмеженим

доступом, оскільки володіє великою важливістю для успішної роботи організації (табл. 1.2).

Таблиця 1.2 – Основні елементи стратегічної інформації

Стратегічні плани	Місія та візія: оформлення основних цілей та бачень організації. Стратегічні завдання: ключові завдання та завдання для досягнення місії.
Сектори діяльності	Визначення пріоритетних сфер роботи: чітка ідентифікація та визначення секторів, на які спрямована діяльність. Розробка стратегій у кожному секторі: плани та стратегії для ефективної реалізації діяльності.
Фінансові плани	Бюджетні призначення: розподіл фінансових ресурсів для виконання стратегічних завдань. Оцінка вартості реалізації стратегії: аналіз фінансових аспектів стратегічних ініціатив.
Забезпечення ресурсами	Людські ресурси: забезпечення достатньої кількості та якості персоналу для реалізації стратегії. Технічні ресурси: забезпечення необхідною технічною інфраструктурою та технологіями.
Внутрішні процеси	Організаційна структура: організація та управління внутрішніми процесами. Методи взаємодії та комунікації: способи співпраці в межах організації та комунікації.
Ризики та можливості	Аналіз ризиків: визначення потенційних загроз та ризиків, що можуть виникнути при реалізації стратегії. Визначення можливостей: розпізнавання можливостей для досягнення стратегічних цілей.
Внутрішні та зовнішні показники ефективності	Ключові показники ефективності (KPI): метрики для вимірювання результатів реалізації стратегії. Оцінка відповідності стратегії завданням: спостереження за тим, наскільки добре стратегія відповідає поставленим завданням.

Стратегічна інформація є основою для прийняття стратегічних рішень та спрямована на забезпечення успішної реалізації місії та завдань організації публічного управління.

4. Технічна інформація органів публічного управління включає в себе дані та деталі, пов'язані із застосуванням технологій та інформаційних систем у роботі організації. Ця інформація може стосуватися технічних засобів, програмного забезпечення, мережевої інфраструктури та інших технічних аспектів, які використовуються для оптимізації робочих процесів та забезпечення ефективної діяльності органів публічного управління (табл. 1.3).

Таблиця 1.3 – Основні компоненти технічної інформації

Інформаційні системи та технології	ERP-системи (Enterprise Resource Planning): інтегровані системи для управління ресурсами організації, включаючи фінанси, кадри, логістику та інше. CRM-системи (Customer Relationship Management): засоби для взаємодії з клієнтами та управління відносинами.
Системи електронного документообігу	Електронні архіви: засоби для зберігання та управління електронними документами. Системи електронного підпису: для підтвердження аутентичності та цілісності електронних документів.
Комп'ютерне обладнання	Сервери та робочі станції: апаратні ресурси для забезпечення роботи інформаційних систем. Периферійні пристрої: друкарки, сканери та інші засоби для обробки та збереження інформації.
Мережева інфраструктура	Локальні та глобальні мережі: забезпечення зв'язку між різними частинами організації та зовнішнім середовищем. Засоби забезпечення безпеки мережі: фаєрволи, антивірусне програмне забезпечення, VPN-з'єднання тощо.
Програмне забезпечення	Офісні пакети: засоби для створення та обробки документів, електронних таблиць, презентацій тощо. Спеціалізовані програми: спеціально розроблені програми для вирішення конкретних завдань, пов'язаних з діяльністю організації.
Електронні платформи та веб-сайти	Електронні громадянські сервіси: Веб-платформи для надання послуг громадянам та підприємствам. Внутрішні та зовнішні веб-сайти: Інформаційні ресурси для комунікації та розповсюдження інформації.
Засоби кібербезпеки	Системи виявлення і запобігання інцидентів безпеки: засоби для виявлення та усунення загроз безпеці інформації. Шифрування даних: заходи для забезпечення конфіденційності та цілісності даних.
Технічна підтримка та сервіси	IT-служба: технічна підтримка для розв'язання проблем, пов'язаних з IT-інфраструктурою. Технічні консультанти: фахівці, які надають поради та консультації з технічних питань.

Ця інформація допомагає органам публічного управління ефективно використовувати технології для покращення своєї роботи та надання якісних послуг громадянам і підприємствам.

Метою інформаційної політики є забезпечення відповідного та безпечного використання інформації для підтримки прийняття рішень і виконання функцій органів управління; регулювання та управління процесами збору, обробки, зберігання, передачі інформації в організації чи системі. Інформаційна політика встановлює принципи, правила, стандарти та

процедури, які визначають, як організація повинна взаємодіяти з інформацією для досягнення своїх стратегічних цілей. Основними цілями інформаційної політики є:

–визначення заходів та стандартів для захисту інформації від несанкціонованого доступу, витоку, втрати або пошкодження;

–визначення правил доступу та обмежень для збереження конфіденційності персональної інформації;

–забезпечення доступності інформації для тих, хто має право на неї, в необхідний момент і в необхідному обсязі;

–визначення процедур та контрольних механізмів для забезпечення цілісності інформації, тобто відсутності її неправомірних змін;

–розподіл ролей та відповідальностей в сфері інформаційної безпеки, включаючи визначення того, хто відповідає за захист та управління інформацією;

–забезпечення відповідності дотримання законодавства, стандартів та внутрішніх правил у сфері обробки інформації;

–підтримка бізнес-процесів;

–визначення принципів етичної обробки інформації та встановлення стандартів поведінки для персоналу та інших зацікавлених сторін;

–визначення процедур та механізмів реагування на інциденти в області інформаційної безпеки.

Цілі спрямовані на створення безпечного, ефективного середовища для обробки та управління інформацією в організації.

Суб'єктом інформаційної політики є той, хто визначає, розробляє та впроваджує стратегії та правила, пов'язані з управлінням інформацією. У контексті органів публічного управління суб'єктом інформаційної політики може бути:

1. Урядові органи: органи влади на різних рівнях (центральний, регіональний, місцевий) визначають політику збору, зберігання, обробки та поширення інформації.

2. Міністерства та департаменти: різні відомства та підрозділи урядових структур можуть мати свої власні політики управління інформацією, спрямовані на виконання їх функцій та завдань.

3. Місцеві органи самоврядування можуть мати свої політики управління інформацією, орієнтовані на потреби конкретних географічних територій.

4. Державні підприємства та установи: суб'єктами можуть бути державні компанії, установи та організації, які регулюють внутрішню інформаційну діяльність.

5. Інші суб'єкти громадянського суспільства: громадські організації, які долучають свої усили для впливу на політику управління інформацією та захисту прав громадян на інформацію.

Суб'єкти інформаційної політики визначають принципи, стандарти, процедури та практики, що стосуються збору, зберігання, обробки та розповсюдження інформації в межах їх повноважень та відповідно до встановлених законів і нормативів.

Цілі інформаційної політики органів публічного управління можуть бути різноманітними і залежать від конкретного контексту, виду організації чи установи. Однак загальні цілі інформаційної політики включають:

– ефективне управління інформацією: забезпечення оптимального використання інформаційних ресурсів для досягнення стратегічних та оперативних цілей організації;

– безпека інформації: захист конфіденційної, критичної та важливої інформації від несанкціонованого доступу, змін та втрати;

– транспарентність та прозорість: забезпечення доступності інформації для стейкхолдерів і громадськості, щоб зміцнити довіру і підвищити прозорість діяльності;

– забезпечення якості інформації: гарантування точності, достовірності та актуальності інформації, що використовується для прийняття рішень;

– впровадження новітніх технологій: заохочення інновацій та використання сучасних технологій для збору, обробки та поширення інформації;

– забезпечення сумісності з вимогами законодавства: виконання вимог щодо обробки та зберігання інформації, які встановлені законами та нормативами;

– підтримка прийняття рішень: забезпечення належного доступу до інформації для прийняття ефективних та обгрунтованих рішень;

– стійкість до кризових ситуацій: розробка механізмів та процедур для збереження доступності інформації навіть в умовах екстрених ситуацій чи криз;

– забезпечення доступності інформації для внутрішніх потреб: впровадження систем для ефективного обміну та використання інформації всередині організації.

Ці цілі можуть варіюватися в залежності від сфери діяльності та завдань конкретної організації чи установи. Реалізація цих цілей сприяє покращенню управління інформацією та сприяє загальному успіху організації.

Засоби інформаційної політики включають різні інструменти, методи та підходи, які використовуються для реалізації інформаційної стратегії та досягнення поставлених цілей. Основні засоби інформаційної політики:

– інформаційні системи та технології: ERP-системи (Enterprise Resource Planning) для інтеграції та управління різними бізнес-процесами; CRM-системи (Customer Relationship Management) для ефективного взаємодії з клієнтами; бізнес-аналітика та звітність для аналізу даних та прийняття управлінських рішень;

– засоби кібербезпеки: антивірусні програми та файрволи для захисту від комп'ютерних загроз; шифрування даних для забезпечення конфіденційності інформації;

– системи управління документами: електронні архіви та системи

документообігу для ефективного управління документами та інформацією;

– засоби електронного урядування (e-Government): електронні платформи та портали для надання електронних послуг та спрощення взаємодії з громадянами та підприємствами;

– політики та стандарти: правила обробки та зберігання інформації для визначення процедур та вимог щодо роботи з даними; стандарти безпеки інформації: забезпечення відповідності безпековим стандартам та вимогам;

– системи моніторингу та аудиту: засоби виявлення порушень безпеки для вчасного виявлення та реагування на можливі загрози; аудиторські системи для відстеження та аналізу використання інформації та дій користувачів;

– освіта та навчання персоналу: програми навчання з кібербезпеки для підвищення обізнаності та навичок персоналу в галузі безпеки інформації;

– методи контролю та аналізу результативності: метрики безпеки інформації для вимірювання ефективності заходів інформаційної політики.

Ці засоби використовуються для розробки, впровадження та підтримки стратегій інформаційної політики з метою забезпечення ефективного та безпечного управління інформацією в органах публічного управління.

Таким чином, теоретичні засади інформаційної політики формують фундаментальну основу для створення систематичного та ефективного підходу до управління інформацією в органах публічного управління. Вони визначають принципи, якими повинні керуватися органи публічного управління для забезпечення високого рівня безпеки, доступності та ефективності в обробці інформації.

1.3. Понятійно-категоріальний апарат інформаційної політики органів публічного управління

По-перше, вважаємо за необхідне проаналізувати поняття «інформаційна політика органів публічного управління» через «державну інформаційну політику». Вважаємо, що цей термін слід розглядати як сукупність конкретних концептуальних уявлень, які взаємоузгоджені та утверджені з урахуванням інтересів і потреб громадян, суспільства та держави в певних сферах життя. Необхідно підкреслити, що об'єкти, суб'єкти, цілі та засоби політики різні [23].

Іванченко Ю. М. зазначав, що державна інформаційна політика – це сукупність основних напрямів і методів діяльності з отримання, використання, поширення та зберігання інформації в країні [3].

На думку Березовської І.Р., «державна інформаційна політика – це така політика, яка має стати основою для вирішення основних завдань суспільного розвитку, а її основним змістом є формування єдиного інформаційного простору в Україні є інтеграція у світовий інформаційний простір для забезпечення інформаційної безпеки людини, суспільства та країни» [4].

Красноступ Г. М. стверджує, що «державна інформаційна політика забезпечується діями, які за своєю суттю є комплексом цілеспрямованих організаційно-правових заходів, що впливають на об’єкти управління (певні національні інтереси) і тим самим дають необхідні результати суспільству [11].

Інформаційна політика органів публічного управління визначає загрози безпеці; формує певний правовий інструментарій; долає загрози з обов’язковим пріоритетом прав людини та свобод громадянина; формує вектор розвитку інформаційного зв’язку. Інформаційна політика є певним правовим статусом, включно з визначенням правових інструментів, і держава використовує ці інструменти для підтримки балансу індивідуальних інтересів, інтересів суспільства та країни в інформаційній сфері та забезпечення інформаційної безпеки.

Вважаємо, що інформаційна політика органів публічного управління –

це напрямок і засіб реалізації комплексу взаємопов’язаних заходів правового та організаційного характеру, спрямованих на отримання, використання, поширення та зберігання інформації, результатом яких є інформаційний процес. Метою впливу на уповноважені суб'єкти (переважно відповідні національні органи) є досягнення необхідних результатів.

Отже, враховуючи проведений аналіз, можна зробити висновок, що в рамках реалізації державної інформаційної політики діяльність уповноважених суб’єктів регулюється правовими нормами щодо застосування різноманітних механізмів отримання, використання, поширення та збереження інформації.

Закон України «Про інформацію», стаття 3, визначає «основні напрями державної інформаційної політики є:

–забезпечення доступу кожного до інформації;

–забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

–створення умов для формування в Україні інформаційного суспільства;

–забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

–створення інформаційних систем і мереж інформації, розвиток електронного урядування;

–постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

–забезпечення інформаційної безпеки України;

–сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору».

Іванченко Ю.М. запропонував наступні основні напрями державної інформаційної політики: «забезпечення доступу громадян до інформації; створення національних інформаційних систем і мереж; зміцнення

матеріально-технічної, фінансово-організаційної, правової та наукової бази; забезпечення ефективного використання інформації; сприяння постійному оновленню, збагаченню та збереженню національних інформаційних ресурсів; створення універсальної системи захисту інформації; сприяння міжнародному співробітництву у сфері інформації та захисту інформаційного суверенітету України; допомога в задоволенні інформаційних потреб українців за кордоном» [3].

Нестеряк Ю., Мельник М. запропонували додати: «забезпечення умов для розвитку та захисту всіх форм володіння інформаційними ресурсами; формування та захист національних інформаційних ресурсів; створення та розвиток центральних і регіональних інформаційних систем і мереж, забезпечення їх сумісності та взаємодії в єдиному національному інформаційному просторі; забезпечення інформаційними ресурсами громадян, державних органів, органів місцевого самоврядування, створення умов для надання організаціями та громадськими об’єднаннями якісної та ефективної інформаційної підтримки; підтримка інформаційних проектів та планів; створення та вдосконалення інвестиційних систем і механізмів сприяння розвитку та реалізації інформаційних проектів; розвиток законодавства у сфері обробки інформації та захисту інформації; гарантування національної безпеки у сфері інформаційних технологій; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем і технологій та засобів їх забезпечення; формування та реалізація єдиної науково-технічної промислової політики у сфері інформаційних технологій з урахуванням рівня розвитку інформаційних технологій у сучасному світі [6; 7; 8].

На думку І.В. Арістової, основною довгостроковою метою державної інформаційної політики України є формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору всієї країни та інтеграції у світовий інформаційний простір. Враховувати національні особливості та інтереси, забезпечуючи при цьому інформаційну безпеку на

внутрішньому та міжнародному рівнях [9; 30].

Соснін О. В. вважає, що основною метою державної інформаційної політики щодо забезпечення національними інформаційними ресурсами є створення необхідних економічних і соціально-культурних умов, а також правових і організаційних механізмів для формування, розвитку та ефективного використання національної інформації, ресурсів в усіх сферах цивільного, громадського та державного життя і діяльності У цьому контексті функції держави в управлінні інформаційними ресурсами можна виділити:

- формування та прийняття політичних рішень, законодавства та нормативно-правових актів щодо забезпечення національної системи управління інформаційними ресурсами та вдосконалення механізмів реалізації правових норм чинного законодавства;

- визначає та реалізує повноваження державних установ, органів регіонального та місцевого самоврядування щодо оперативного управління (володіння, розпорядження, користування) державними інформаційними ресурсами;

- розробка та реалізація організаційних заходів, а також нормативно-методичне забезпечення діяльності відомчих, регіональних органів та громадських організацій у сфері формування та використання інформаційних ресурсів за умови координації діяльності зазначених органів;

- розробка та застосування фінансово-економічних засад регулювання формування та використання інформаційних ресурсів;

- державна реєстрація інформаційних ресурсів для забезпечення цілісності, організації вихідних та похідних інформаційних ресурсів, створених державними органами, органами місцевого самоврядування, підприємствами, установами на основі інформації, яка формується у процесі діяльності незалежно від форми власності;

- запровадження техніко-методологічних єдиних засад формування інформаційних ресурсів за результатами діяльності державних органів,

органів місцевого самоврядування, державних підприємств і організацій у вільному доступі для громадян та організацій (крім інформаційних ресурсів), що містять відомості, що є державною таємницею, та інша інформація з обмеженим доступом із захищеним доступом);

- забезпечує ефективне використання інформаційних ресурсів у діяльності державних установ, органів місцевого самоврядування, а також державних підприємств, установ та організацій;

- оптимізація державної інформаційної політики та забезпечення науково-технологічних, виробничо-технологічних та організаційно-економічних умов для створення та застосування інформаційних технологій та інших елементів інформаційної інфраструктури для формування, розвитку та ефективного використання інформаційних ресурсів для сприяння доступу громадян до глобальних інформаційних ресурсів і глобальних інформаційних систем;

- забезпечення функціонування ефективної інтегрованої системи захисту інформаційних ресурсів;

- забезпечує захист громадян, суспільства та країни від неправдивої, спотвореної та недостовірної інформації;

- розроблення та впровадження правових, організаційних та економічних механізмів щодо форм і засобів руху інформаційних ресурсів в Україні (інформаційних ринків, інформаційних технологій, засобів обробки інформації та інформаційних послуг);

- стандартизація інформаційного співробітництва для забезпечення рівноправного та взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну, реалізації єдиної національної політики та наукового забезпечення формування, розвитку та використання національних інформаційних ресурсів у національній системі управління;

– кадрове забезпечення функціонування національної системи управління національними інформаційними ресурсами;

– здійснення інформаційно-аналітичного забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами;

- встановлення порядку і правил контролю за формуванням, розвитком і використанням інформаційних ресурсів;

- контроль за формуванням, розвитком, використанням інформаційних ресурсів у сфері публічно-інформаційних відносин та дотриманням законодавства у сфері судового управління [10].

Пахнін М. Л. стверджує, що «державна інформаційна політика має ґрунтуватися на таких основних принципах:

- відкритість – усі основні заходи інформаційної політики мають відкрито обговорюватися суспільством;

- рівність інтересів – політика, яка однаково враховує інтереси всіх учасників інформаційної діяльності, незалежно від їх статусу в суспільстві та форми власності («правила гри» однакові для всіх);

- системність – при реалізації рішення про зміну статусу одного з об'єктів регулювання необхідно враховувати його загальний вплив на стан інших об'єктів та на зміни статусу всіх об'єктів;

- пріоритет надається місцевим виробникам - за рівних умов пріоритет надається конкурентним місцевим виробникам інформаційно-комунікаційних засобів, продукції та соціального позиціонування - основні заходи державної інформаційної політики мають бути спрямовані на забезпечення соціальних інтересів громадян України;

- патріотизм – усі заходи щодо розвитку інформаційного поля мають реалізовуватися на основі захисту національних інтересів;

- юридичний пріоритет – формулювання та впровадження законів і нормативних актів мають пріоритет над будь-якою формою вирішення проблем в інформаційній сфері [11, с.3].

Закон України «Про інформацію» може бути оновлений з урахуванням двох глобальних напрямів державного управління інформаційною сферою в умовах розвитку інформаційних технологій:

1) інформаційно-технологічний напрям розглядає такі рішення, як створення технологічної бази для переходу України до інформаційного суспільства, розвиток інформаційно-комунікаційних технологій, розвиток, використання та впровадження форм діяльності на основі ІКТ.

Інформаційно-технологічний напрям інформаційної політики органів публічного управління визначає стратегії та дії в сфері використання інформаційних технологій для забезпечення ефективності, прозорості та якості діяльності органів влади. Цей напрям охоплює величезний спектр аспектів:

1.1.Електронне урядування (e-government): розвиток та впровадження інформаційних технологій для надання громадянам та підприємствам доступу до послуг та ресурсів уряду в електронному вигляді (наприклад, електронні портали, онлайн-сервіси, електронні форми звернень тощо).

1.2.Інформаційна безпека: заходи з забезпечення захисту інформації, яка обробляється та зберігається органами публічного управління (технічні, організаційні та правові заходи для запобігання несанкціонованому доступу, витоку інформації та інших загроз).

1.3.Автоматизація та оптимізація процесів: використання інформаційних технологій для автоматизації та оптимізації внутрішніх та зовнішніх процесів управління та надання послуг.

1.4.Впровадження інновацій: використання новітніх технологій, таких як штучний інтелект, блокчейн, аналітика даних та інші, для вдосконалення роботи органів влади.

1.5.Відкриті дані (open data): розміщення певної інформації в обробленому та доступному для загального використання форматі з метою створення нових можливостей для громадськості та бізнесу.

1.6.Цифрова трансформація: загальний перехід органів управління до використання цифрових технологій для покращення всіх аспектів їхньої діяльності, включаючи взаємодію з громадськістю, внутрішні процеси та прийняття рішень.

1.7.Інформаційна інфраструктура: розвиток та підтримка інформаційної інфраструктури, включаючи мережі зв'язку, централізовані системи зберігання даних, хмарні технології та інше.

Цей напрям інформаційної політики є важливим для того, щоб органи публічного управління могли ефективно використовувати інформаційні технології для вдосконалення своєї діяльності та взаємодії з громадськістю.

2) інформаційно-змістовний напрям інформаційної політики органів публічного управління пов'язаний з діяльністю засобів масової комунікації; вирішує соціальні та правові обов’язки ЗМІ перед суспільством; захищає інформаційні права та свободи громадян; визначає стратегії, підходи та процеси, пов'язані з формуванням, обробкою, передачею та використанням інформації для досягнення стратегічних цілей та завдань; наповнює внутрішній та міжнародний простір позитивною інформацією про Україну. Основні аспекти цього напряму:

2.1. Інформаційна транспарентність: забезпечення доступу до інформації для громадськості та інших зацікавлених сторін з метою забезпечення прозорості та відкритості у діяльності органів влади.

Комунікаційна стратегія: розроблення плану спілкування та комунікаційних стратегій для ефективної взаємодії з громадськістю, ЗМІ та іншими зацікавленими сторонами.

2.2. Інформаційна політика в сфері освіти: розвиток та впровадження програм та ініціатив з підвищення інформаційної грамотності серед громадян для забезпечення їх здатності розуміти та використовувати інформацію.

2.3. Забезпечення якості інформації: розробка стандартів та процедур для забезпечення точності, достовірності та актуальності інформації, яку надають органи управління.

2.4. Доступ до публічної інформації: гарантування права громадян на доступ до публічної інформації, включаючи офіційні документи, рішення та інші матеріали.

2.5. Інформаційна підтримка прийняття рішень: забезпечення органів управління інформацією, необхідною для прийняття обгрунтованих рішень, в тому числі аналітичною та статистичною інформацією.

2.6. Медійна політика: розробка стратегій взаємодії з ЗМІ та керування власним образом в засобах масової інформації.

2.7. Організація та зберігання інформації: розробка систем для організації та зберігання великої кількості інформації, включаючи бази даних та інші інформаційні ресурси.

Цей напрям інформаційної політики покликаний забезпечити ефективне управління інформацією, яка генерується та використовується органами публічного управління, і зробити цю інформацію доступною, зрозумілою та корисною для громадськості та інших сторін.

Таким чином, оптимізація адміністративного законодавства регулює всі аспекти захисту інформаційного простору органів публічного управління від негативної інформації, необхідно відповідним чином доповнити перелік основних напрямів національної інформаційної політики, що міститься в Законі України «Про інформацію» полягає в наступному: сприяння формуванню ринків інформаційних ресурсів, послуг, інформаційних систем і технологій та засобів їх забезпечення; розвиток адміністративного законодавства у сфері обробки інформації, інформатизації та захисту інформації (у тому числі запровадження законодавчої бази відповідно до міжнародних стандартів у цій сфері); супровід проектів і планів інформатизації; правовий нагляд за функціонуванням міжнародної інформаційної системи України (особливо мережі інтернет); сприяння процесу створення та розвитку в країні відкритого інформаційного суспільства; подальший розвиток інформаційного законодавства як самостійної галузі права тощо.

Висновки до першого розділу

Основні елементи методології включають: чітке визначення об'єкта та мети дослідження, а також конкретизація питань, на які слід знайти відповіді; роз'яснення основних термінів, концепцій та засад, які використовуються в дослідженні, для уникнення непорозумінь та забезпечення однозначності термінології; визначення та обґрунтування вибору конкретних методів збору та аналізу даних, таких як опитування, аналіз документів, експертні оцінки, статистичний аналіз, тощо; розробку інструментів для збору та обробки даних, включаючи анкети, опитувальники, програмне забезпечення, що використовується для обробки інформації; визначення етичних стандартів та принципів, які слід дотримуватися під час проведення дослідження; визначення меж дослідження та визначення обсягу вивчення конкретних аспектів інформаційної політики; визначення підходів до аналізу даних, які можуть бути кількісними, якісними чи комбінованими, залежно від характеру дослідження; визначення можливих ризиків та невизначеності, які можуть виникнути під час дослідження, та розробка стратегій їх управління; розробку механізмів для перевірки достовірності та надійності зібраних даних, а також обґрунтування їх валідності; розробку методів аналізу отриманих даних та їх інтерпретація в контексті висновків дослідження; формулювання висновків на основі проведеного дослідження та розробка рекомендацій для подальших дій.

Методологія дослідження є каркасом, який допомагає забезпечити наукову обґрунтованість, системність та об'єктивність дослідження інформаційної політики органів публічного управління.

Політичні та соціально-економічні процеси в нашій державі змінюють правове регулювання відносин в інформаційній сфері, ефективність формування інформаційної культури населення та відповідального ставлення до використання інформаційного простору; оптимізують системи управління інформаційними ресурсами на національному та індивідуальному рівнях.

РОЗДІЛ 2
АНАЛІТИКО-ДОСЛІДНИЦЬКІ ВИМІРИ НАПРЯМІВ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ

2.1. Нормативно-правове забезпечення інформаційної політики органів публічного управління в Україні

Процес суспільних і національно-демократичних перетворень потребує правового забезпечення, що зумовлює реформування всієї правової системи України, починаючи з реформування законодавства, оскільки в чинному законодавстві України є великі недоліки.

Враховуючи різноманітність нормативно-правових актів, що регулюють суспільні відносини у сфері інформаційної політики в Україні, вважаємо за необхідне проаналізувати концептуальні акти [17].

Під нормативно-правовими положеннями про інформаційну безпеку в Україні розуміють форму сильного правового впливу на суспільні інформаційні відносини, що застосовуються державою для організації, закріплення та забезпечення публічних інформаційних відносин [18].

На сьогодні одним із важливих напрямків стратегії адміністративно-правового регулювання інформаційної безпеки України є аналіз та вдосконалення нормативно-правового забезпечення цієї сфери.

Забезпечення інформаційної політики органів публічного управління в Україні, тобто безпеки її національних інтересів в інформаційній сфері, передбачає першочерговий розвиток системи нормативно-правових норм відносин у цій сфері, реагування на загрози цим інтересам та спрощення відповідних законодавчих процедур.

Інформаційна політика органів публічного управління в Україні

регулюється рядом законів та інших нормативно-правових актів:

Закон України «Про інформацію» (1992 р.) «регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації»; визначає загальні принципи забезпечення доступу до інформації та використання неї.

Закон України «Про доступ до публічної інформації» (2011 р.) «визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес»; регулює питання доступу громадян до публічної інформації, обов'язки органів публічної влади щодо надання інформації тощо [24].

Закон України «Про захист персональних даних» (2010 р.) «регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних; поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів»; визначає правові засади захисту персональних даних громадян.

Концепція розвитку електронного урядування в Україні (2017 р.) визначає шляхи розвитку та вдосконалення електронного урядування, в тому числі в сфері інформаційної політики. «Метою Концепції є визначення напрямів, механізмів і строків формування ефективної системи електронного урядування в Україні для задоволення інтересів та потреб фізичних та юридичних осіб, вдосконалення системи державного управління, підвищення конкурентоспроможності та стимулювання соціально-економічного розвитку країни».

Міжнародна ініціатива «Партнерство «Відкритий Уряд» (2011 р.) визначає ключові зобов'язання країн-учасниць: «підвищення доступності інформації про діяльність державних органів; підтримка залучення громадянського суспільства; впровадження високих стандартів професійної чесності у державному управлінні; підвищення рівня доступу до нових технологій задля забезпечення відкритості та підзвітності».

Партнерство «Відкритий Уряд» відіграло ключову роль в процесі для розвитку політики відкритих даних в Україні. Зокрема, внесення змін до Закону України «Про доступ до публічної інформації» та прийняття Постанови КМУ №835 від 21 жовтня 2015 року було передбачене планом дій в рамках партнерства. Згодом стали відкритими декларації держслужбовців, бюджетні трансакції, дані про власників компаній [24].

Ініціатива «Партнерство «Відкритий Уряд» в Україні є частиною стратегії електронного урядування та реформи публічного сектору. Ця ініціатива спрямована на забезпечення більшої відкритості, прозорості та взаємодії між державними органами, громадянами та бізнесом. Деякі ключові аспекти ініціативи «Партнерство «Відкритий Уряд» включають:

– розширення доступу до електронних послуг для громадян та бізнесу, спрощення процедур та поліпшення якості надання послуг;

– забезпечення доступу до великого обсягу відкритих даних державних органів, що сприяє створенню умов для розвитку нових сервісів та продуктів;

– впровадження механізмів для забезпечення прозорості та відкритості діяльності державних органів, включаючи публікацію інформації про бюджет, рішення та інші аспекти роботи;

– залучення громадян до участі в прийнятті рішень через електронні консультації та голосування;

– забезпечення кібербезпеки в системі електронного урядування для захисту інформації та персональних даних;

– впровадження стандартів та практик, які сприяють

інтероперабельності систем та обміну даними між різними органами.

Ця ініціатива є частиною стратегії розвитку електронного урядування та має на меті створення сприятливого середовища для розвитку цифрової економіки та покращення якості надання послуг громадянам і бізнесу. Будь ласка, перевірте офіційні джерела для отримання останньої інформації про ініціативу.

«У рамках членства України в міжнародній Ініціативі «Партнерство «Відкритий Уряд» Секретаріатом Кабінету Міністрів було організовано розроблення шостого національного плану дій. Протягом січня – травня 2023 р. проведено 11 публічних онлайн-обговорень та узгоджувальних нарад за участю представників інститутів громадянського суспільства, органів виконавчої влади, науковців, експертів. За результатами був розроблений проект розпорядження Кабінету Міністрів України «Про затвердження плану дій із впровадження Ініціативи «Партнерство «Відкритий Уряд» у 2023 – 2025 роках», який оприлюднювався для електронних консультацій на Урядовому порталі» [25].

«Концепція розвитку електронного урядування в Україні (2017 р.) визначає напрями, механізми і строки формування ефективної системи електронного урядування в Україні для задоволення інтересів та потреб фізичних та юридичних осіб, вдосконалення системи державного управління, підвищення конкурентоспроможності та стимулювання соціально-економічного розвитку країни» [30].

«Реалізація Концепції здійснюється за такими основними принципами: цифровий за замовчуванням – забезпечення будь-якої діяльності органів влади (у тому числі надання публічних послуг, забезпечення міжвідомчої взаємодії, взаємодії з фізичними та юридичними особами, інформаційно-аналітичної діяльності) передбачає електронну форму реалізації як пріоритетну, а планування та реалізацію будь-якої реформи, проекту чи завдання – із застосуванням інформаційно-комунікаційних технологій; одноразове введення інформації – реалізація підходу, за якого фізичні та

юридичні особи лише один раз подають інформацію до органів влади, а у подальшому ця інформація повторно використовується органами влади для надання публічних послуг та виконання інших владних повноважень з дотриманням вимог захисту інформації та персональних даних; сумісність за замовчуванням – здійснення проектування та функціонування інформаційно-телекомунікаційних систем в органах влади відповідно до єдиних відкритих вимог та стандартів для забезпечення їх подальшої сумісності та електронної взаємодії та повторного використання; доступність та залучення громадян; відкритість та прозорість; довіра та безпека» [30].

Закон України «Про Національну програму інформатизації» (2022 р.) регулює правові відносини, що виникають під час формування та виконання Національної програми інформатизації [30].

«Національна програма інформатизації – це комплекс завдань, програм, проектів, робіт з інформатизації, спрямованих на розвиток інформаційного суспільства шляхом концентрації та раціонального використання фінансових, матеріально-технічних та інших ресурсів, виробничого і науково-технічного потенціалу держави, координації діяльності державних органів, органів місцевого самоврядування, а також підприємств, установ, організацій незалежно від форми власності.

Національна програма інформатизації визначає особливості реалізації державної політики у сфері інформатизації для забезпечення потреб та розвитку інформаційного суспільства, впровадження інформаційно-комунікаційних та цифрових технологій» [29].

Закон України «Про науково-технічну інформацію» визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни. Метою Закону є створення в Україні правової бази для одержання та використання науково-технічної інформації. Законом регулюються правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та

поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі. Дія Закону поширюється на підприємства, установи, організації незалежно від форм власності, а також громадян, які мають право на одержання, використання та поширення науково-технічної інформації. Дія Закону не поширюється на інформацію, що містить державну та іншу охоронювану законом таємницю» [27].

Закон України «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України [23].

Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші державні органи, в тому числі територіальні органи центрального органу виконавчої влади, що реалізує державну митну політику, та центрального органу виконавчої влади, що реалізує державну податкову політику, утворені як відокремлені підрозділи центрального органу виконавчої влади без статусу юридичної особи, Верховну Раду Автономної Республіки Крим, Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі - державні органи, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці. Передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом. У разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, установлено інші, ніж передбачені цим Законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору України [23].

Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». «Стратегія інформаційної безпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних. Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина» [72]. «Досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки» [72].

Указом Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року затверджено «Стратегію кібербезпеки України», яка сприятиме подальшій розбудові національної системи кібербезпеки на засадах стримування, кіберстійкості, враховуючи наступні взаємодії: «посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале

функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість); забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами - членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія) [73].

Україна, крім основних суб'єктів національної системи кібербезпеки, залучить до вирішення завдань у цій сфері більш широке коло учасників, у тому числі суб'єктів господарювання, громадські об'єднання та окремих громадян України. Ключову об'єднувальну та координаційну роль у цьому процесі відіграватиме Національний координаційний центр кібербезпеки» [73].

Закон України «Про медіа» (2023 р.) «спрямований на забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, на забезпечення плюралізму думок і вільного поширення інформації, на захист національних інтересів України та прав користувачів медіа-сервісів, регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності і незалежності медіа та визначає правовий статус, порядок формування, діяльності та повноваження Національної ради України з питань телебачення і радіомовлення» [22].

Така велика кількість нормативно-правових актів свідчить про те, що влада сподівається повноцінно та комплексно контролювати інформаційне поле та закласти необхідний мінімум для ефективної реалізації інформаційної політики.

Ці закони та акти спрямовані на забезпечення прозорості, відкритості

та ефективності в управлінні інформацією в органах публічного управління. Важливо зазначити, що законодавство може змінюватися, тому рекомендується перевіряти останній стан законодавства для отримання актуальної інформації.

Норми права складають основу забезпечення інформаційної безпеки та визначають ефективність діяльності держави, суспільства та окремих громадян в інформаційній сфері щодо захисту національних інтересів України. До складу бази даних входять міжнародно-договірні норми України, закони України, акти Президента України, постанови уряду, нормативні акти державних органів, що регулюють відносини у цій сфері [12].

Спеціальними нормативними законами та підзаконними актами регулюються такі питання, як забезпечення інформаційної безпеки, захист інформації, охорона державної таємниці, забезпечення конфіденційності інформації та захист інформаційних ресурсів з метою реалізації положень доктрин індивідуальної, національної та громадської безпеки.

Кількісний пріоритет нормативно-правових заходів, спрямованих на регулювання інформаційної та технологічної безпеки, над інформацією у сфері прав і свобод, а також психологічною та інформаційною безпекою є очевидним, і ми вважаємо, що це пов’язано з поглибленим розвитком інформаційної безпеки. технологія і, отже, необхідність цієї сфери реагувати на зміни в певних стандартах.

Особливим недоліком українських нормативно-правових актів з питань інформаційної політики є їх розпорошеність у численних нормативно-правових актах з різною юридичною силою. Крім того, важливі питання регулюються підзаконними актами.

Не менш важливою проблемою для ефективного забезпечення інформаційної безпеки в Україні є невідповідність нормативно-правових актів чинній Конституції.

Для національного інформаційного законодавства характерним є

декларативний характер великої кількості норм, без конкретизації порядку їх застосування, через що ступінь правової реалізації правових норм, що регулюють сферу суспільних відносин, є низьким. Забезпечення інформаційної безпеки. Крім того, існує велика кількість загальних або довідкових правових норм, дуже абстрактних і суб'єктивних понять, які вимагають формального тлумачення або чіткого визначення, а також відсутність твердих основних визначень (таких як інформаційна безпека) є джерелами загроз інформаційній політики в Україні.

Аналізуючи нормативно-правові акти у сфері інформаційної політики в Україні, можна зробити висновок, що інформаційне законодавство потребує вдосконалення.

2.2. Зарубіжний досвід розвитку інформаційної інфраструктури органів публічного управління

Регулювання інформаційної політики є складним завданням, і різні країни мають різні підходи до цього питання. Глобальна інформаційна інфраструктура є сукупністю технічних, організаційних та нормативних елементів, які забезпечують глобальний обмін інформацією між різними точками світу. Зарубіжний досвід регулювання інформаційної інфраструктури ґрунтується на кількох фундаментальних принципах:

1. Доступність до публічної інформації та універсальність: Забезпечення рівного доступу до інформаційних ресурсів та послуг для всіх користувачів, незалежно від їхнього місця проживання, соціально-економічного статусу чи інших обставин.

Багато країн розробляють закони, які гарантують доступ громадськості до публічної інформації. Наприклад, в Швеції та Норвегії існують прогресивні закони про доступ до інформації, що сприяють відкритості та

прозорості владних структур.

2. Інтероперабельність: створення систем та технологій, які можуть взаємодіяти та обмінюватися інформацією без обмежень, незалежно від виробника чи конкретної технічної реалізації. Інтероперабельність в інформаційному контексті в європейських країнах є ключовим аспектом для забезпечення ефективного функціонування та взаємодії різних систем та служб. В країнах ЄС існують ініціативи та стратегії для підтримки інтероперабельності в різних сферах:

– електронне урядування (e-Government) для полегшення взаємодії громадян, бізнесу та владних органів; стандартизація та використання відкритих стандартів відіграють важливу роль у забезпеченні інтероперабельності між різними системами та платформами;

– європейська цифрова інфраструктура, яка включає в себе проекти з підтримки широкої доступності, інтероперабельності та безпеки електронних послуг;

– єдина цифрова платформа для доступу до послуг Європи (Connecting Europe Facility (CEF Digital) спрямована на забезпечення інтероперабельності між різними системами електронного урядування в країнах ЄС на 2021-2027 роки; орієнтована підтримку та залучення державних та приватних інвестицій в об’єкти критичної інфраструктури (електромережі, транспортні мережі та інформаційно-комунікаційні системи);

– Європейська Комісія підтримує стандартизацію в різних галузях, щоб забезпечити взаємодію та обмін даними між різними системами та країнами;

– ініціативи щодо підтримки цифрової інтероперабельності між країнами ЄС, які сприяють формуванню загального розуміння проблем кібербезпеки та сприяє спільним зусиллям у вирішенні цих проблем на міжнародному рівні.

Ці заходи та ініціативи спрямовані на створення спільного підходу до

інтероперабельності в різних сферах, таких як електронне урядування, цифрова інфраструктура та інші електронні послуги. Це сприяє покращенню спільних стандартів та ефективному обміну інформацією між різними національними системами в Європі.

3. Інформаційна безпека та конфіденційність: захист інформації від несанкціонованого доступу, витоків та інших загроз, забезпечення конфіденційності особистої інформації користувачів. Країни розвивають стандарти та стратегії забезпечення інформаційної безпеки. Сполучені Штати, наприклад, активно працюють над заходами з кіберзахисту та протидії кіберзлочинності, оскільки це стає все більш актуальним у сучасному цифровому середовищі. Проаналізуємо ключові засади роботи органів публічного управління з кіберзахисту та протидії кіберзлочинності в США:

Агентство з кібербезпеки та захисту інфраструктури (Cybersecurity and Infrastructure Security Agency (CISA) [https://www.cisa.gov/]: створене для забезпечення захисту критичної інфраструктури та підтримки агентств у реагуванні на кіберзагрози. CISA надає інформацію про найкращі практики кібербезпеки у визначенні критичної інфраструктури, щоб допомогти державним, місцевим і галузевим установам, окремим особам і організаціям впроваджувати профілактичні заходи та керувати кіберризиками.

Кіберкомандування США (United States Cyber Command) [https://www.cybercom.mil/]: військова одиниця, яка відповідає за кіберзахист та відповідь на кіберзагрози.

Національна кіберстратегія Міністерства оборони на 2023 рік (National Cyber Strategy) [https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf]: визначає основні принципи та стратегії кібербезпеки для захисту національних інтересів; визначає, як Міністерство працюватиме в кіберпросторі, щоб захистити американський народ і просувати пріоритети національної оборонної стратегії Сполучених Штатів: захист країни, враховуючи

зростаючу багатодоменну загрозу з боку КНР; стримування стратегічних нападів на Сполучені Штати, союзників та партнерів; стримування агресії, водночас готовність до перемоги в конфлікті, коли це буде необхідно, – пріоритетність викликів КНР в Індо-Тихоокеанському регіоні та росії в Європі; створення стійких об'єднаних сил і оборонної екосистеми.

Один із найбільш відомих документів для зміцнення кібербезпеки в США став Указ Президента Трампа від 11 травня 2017 року під назвою «Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure» (Екзекутивний Указ щодо зміцнення кібербезпеки федеральних мереж та критичної інфраструктури), який зосереджує федеральні зусилля на модернізації федеральної інфраструктури інформаційних технологій, співпраці з державними та місцевими органами влади та партнерами з приватного сектору для повнішого захисту критичної інфраструктури та співпраці з іноземними союзниками [http://surl.li/orwus].

Цей Указ орієнтований на поліпшення захисту кібербезпеки урядових систем та критичної інфраструктури має наступні ключові положення:

забезпечення безпеки та захисту федеральних інформаційних систем;

–визначення стандартів та процедур для кібербезпеки федеральних мереж та інформаційних систем;

–запровадження заходів для попередження, виявлення та відповіді на кіберзагрози;

–співпраця з приватним сектором та іншими стейкхолдерами для поліпшення кібербезпеки;

–підвищення кваліфікації персоналу в сфері кібербезпеки через навчання та розвиток;

–вдосконалення заходів для захисту критичної інфраструктури в Сполучених Штатах.

Цей та інші екзекутивні укази ставлять за мету посилення заходів у сфері кібербезпеки, зокрема в урядових агентствах та критичних секторах економіки. Призначення та специфікації екзекутивних указів можуть

змінюватися залежно від конкретної адміністрації та її пріоритетів.

4. Захист приватності: деякі країни активно працюють над законодавством, яке забезпечує захист особистої інформації громадян. Зокрема, Європейський Союз впровадив 25 травня 2018 року «Загальний регламент з питань захисту даних (General Data Protection Regulation, GDPR)» [https://gdpr-info.eu/], який надає громадянам більший контроль над своєю особистою інформацією. Цей регламент призначений для захисту особистих даних громадян ЄС та регулює обробку таких даних організаціями та підприємствами. GDPR спрямований на створення єдиної системи правил для захисту особистих даних у всьому Європейському Союзі, незалежно від того, де розташована організація, яка обробляє ці дані. Він покликаний поліпшити приватність та безпеку особистих даних та відповідати сучасним викликам цифрового світу.

5. Електронне урядування. Багато країн активно впроваджують електронне урядування для поліпшення надання послуг та спрощення взаємодії між громадянами та урядовими органами.

Франція виявляє активний інтерес до розвитку електронного урядування (e-government) з метою поліпшення доступу до публічних послуг, оптимізації управління та спрощення взаємодії між урядовими органами та громадянами запроваджено: платформу для ідентифікації та автентифікації громадян платформу «FranceConnect» [https://franceconnect.gouv.fr/], яка дозволяє користувачам отримувати доступ до різних публічних служб, використовуючи єдині авторизаційні дані; портал публічних послуг «Service-Public.fr» [https://www.service-public.fr/] для надання інформації про публічні послуги та права громадян; Цифровий центр правосуддя (Centre Numérique de la Justice), який є ініціативою, спрямованою на модернізацію та цифровізацію судової системи. Цей центр має на меті впровадження сучасних технологій та електронних рішень для полегшення доступу до юридичних послуг та оптимізації процесів в системі правосуддя. Центр допомагає зробити правосуддя більш відкритим, доступним та відповідним

сучасним технологічним вимогам.

Уряд Швеції активно використовує інформаційні технології для поліпшення надання публічних послуг та спрощення взаємодії між громадянами, підприємствами та урядовими органами. Швеція пропонує широкий спектр електронних послуг для громадян і бізнесу, таких як: електронне подання податкових декларацій, заявок на допомогу, онлайн-терміни в органах влади тощо; використовує ефективні системи ідентифікації та безпеки для забезпечення конфіденційності та безпеки особистих даних; використовує електронні системи для покращення доступу до медичних послуг, обміну медичною інформацією та надання соціальної допомоги; здійснює експерименти щодо впровадження електронного голосування та інших цифрових методів участі у громадському житті. Єдиний портал урядових послуг «Verksamt.se» [https://www.verksamt.se/] надає інформацію та електронні послуги для підприємців, спрощуючи процеси реєстрації та управління бізнесом.

6. Деякі країни активно використовують концепцію відкритих даних для забезпечення доступу до інформації для громадськості та підтримки інновацій. Велика Британія та Канада – країни, де відкриті дані використовуються для стимулювання розвитку нових продуктів та послуг.

Відкриті дані в Канаді визначаються та регулюються за концепцією «Відкритий уряд Канади» (Canada Open Government) [https://open.canada.ca/en/using-open-data], яка базується на принципах відкритості, доступності (легкий доступ до даних), та використання (можливість використання та повторного використання даних).

Інформація урядових організацій Канади публікується на власних порталах даних та на централізованому порталі відкритих даних Канади (data.gc.ca), що сприяє їхньому поширенню. Для полегшення використання та обробки даних рекомендується використовувати відкриті стандарти та формати, такі як CSV, JSON, XML тощо. Відкриті дані в Канаді розглядаються як ключовий інструмент для стимулювання інновацій,

розвитку нових технологій та сприяння громадському участь у демократичних процесах.

Велика Британія активно працює над впровадженням концепції відкритих даних для забезпечення доступу громадськості до інформації та сприяння інноваціям та розвитку. Велика Британія має свій власний централізований портал відкритих даних – «data.gov.uk», де різні урядові організації публікують свої дані для громадськості; рекомендує використання ліцензій, які забезпечують вільний доступ та можливість повторного використання даних без обмежень.

7. Стратегії цифрової трансформації для вдосконалення ефективності державного управління та підвищення рівня обслуговування громадян.

ЄС розробляє та впроваджує ряд стратегій та ініціатив у сфері цифрової трансформації, включаючи програми «Цифровий єдиний ринок» (Digital Single Market) [http://surl.li/orxhg] та «Цифрова Європа» (Digital Europe) [https://www.digitaleurope.org/].

Німеччина має свою національну стратегію цифрової трансформації, в якій надається пріоритет розвитку цифрових технологій та інновацій.

Франція активно працює над цифровою трансформацією, впроваджуючи стратегію «France Digital» [https://francedigitale.org/en] та інші ініціативи для підтримки цифрового розвитку.

Сінгапур має амбіційні плани щодо цифрової трансформації та створення «Smart Nation» за допомогою інновацій та цифрових технологій. «Smart Nation» [https://www.smartnation.gov.sg/] - це стратегічна ініціатива Сінгапуру, спрямована на впровадження технологій та інновацій для створення інтелектуального та ефективного суспільства (99% державних послуг є цифровими). Ця ініціатива призначена для використання технологій для поліпшення якості життя громадян, оптимізації роботи уряду, розвитку бізнесу та забезпечення сталого розвитку.

Індія розвиває національну стратегію «Digital India» [https://www.digitalindia.gov.in/], спрямовану на вдосконалення цифрової

інфраструктури; розвиток цифрових послуг та забезпечення доступу до електронних послуг для громадян.

Китай розвиває платформу ««Цифровий шовковий шлях» (Digital Silk Road), яка означає розвиток інтерконтинентальних цифрових зв'язків, обмін даними та співпрацю в галузі технологій. Платформа покликана усунути низку складнощів у міжнародній торговій системі. Функціональність платформи дозволить відстежувати транзакції та максимально скоротити всі процедури, при цьому забезпечуючи максимальну безпеку та надійність. Як результат, завдяки Digital Silk Road інтенсивність міжнародної торгівлі у регіоні зросте ще більше.

Китай активно працює над ініціативами, спрямованими на створення глобальної цифрової інфраструктури, яка об'єднує різні регіони світу (наприклад, побудова цифрових мереж, електронних комунікаційних магістралей та інших технологічних інфраструктурних проектів).

Таким чином, дослідження зарубіжного досвіду сприяє розвитку міжнародної співпраці в сфері інформаційної політики, обміну досвідом та створення стандартів. Ефективність інформаційної політики часто визначається не тільки національними підходами, але й глобальною співпрацею. Країни постійно вдосконалюють свої підходи до інформаційної політики, враховуючи нові виклики та можливості, що виникають у зв'язку з швидким розвитком технологій та змінами в суспільстві.

2.3. Практичні рекомендації щодо удосконалення інформаційної політики України в умовах війни

Державна інформаційна політика повинна закласти основи для вирішення фундаментальних завдань розвитку суспільства, головними з яких є формування єдиного інформаційного простору України та її входження у світовий інформаційний простір, гарантування інформаційної безпеки особистості, суспільства й держави [7]. Інформаційна політика в її сучасному розумінні є інструментом забезпечення безпеки людини, суспільства, держави, а також світової спільноти.

Важливими завданнями інформаційної політики в умовах війни має стати вирішення проблеми балансу інтересів суспільства, отримання об'єктивної та своєчасної інформації, та необхідність дотримання вимог секретності в умовах ведення масштабних бойових дій. Виконання різноманітних завдань збройними силами та іншими мілітаризованими формуваннями з відбиття агресії ворога.

Інформаційна політика в умовах війни – це система заходів, що здійснюються державою спільно з інститутами громадянського суспільства щодо регулювання інформаційних процесів, формування та розвитку інформаційного суспільства на основі пріоритету національних інтересів країни в сфері її оборони, з метою захисту прав та інтересів людини, моральних цінностей, забезпечення інформаційної безпеки особистості, суспільства та самої держави [1].

Стійкість та міцність соціальної системи пропорційна ступеню узгодженості дій органів державного управління та медіа, що забезпечує прямий та зворотний зв'язок між громадянським суспільством та державою. Війна та агресивна інформаційна політика агресора спрямована на формування переконання про нестабільність, погіршення соціально-економічної обстановки, активізує деструктивні політико-ідеологічні фактори, що становлять небезпеку для системи національних цінностей, ідеалів, традицій, що руйнують структури соціалізації особистості та створюють загрозу безпеці життєдіяльності людини, суспільства та держави.

Важливим кроком у процесі формування організаційно-правових аспектів державної інформаційної політики в умовах війни є Закон України «Про медіа» від 13 грудня 2022 року № 2849-IX, який «…спрямований на забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, на забезпечення плюралізму думок і вільного поширення інформації, на захист національних інтересів України та прав користувачів медіа-сервісів, регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності і незалежності медіа та визначає правовий статус, порядок формування, діяльності та повноваження Національної ради України з питань телебачення і радіомовлення...» До серйозних порушень законодавства про інформацію цей Закон відносить: поширення інформації, яка наголошує на тому, що збройна агресія проти України є внутрішнім конфліктом, громадянською війною або громадянською війною, якщо вона є наслідком розпалюванням ворожнечі чи ненависті або закликами до насильницьких змін, повалення конституційного ладу чи порушення територіальної цілісності; поширення неправдивих матеріалів щодо збройної агресії та дій держави-агресора (держави-окупанта) та її посадових осіб, осіб і організацій, підконтрольних державі-агресору (державі-окупанту), якщо її наслідками є розпалювання ворожнечі чи ненависті або закликають до насильницької зміни чи повалення. порушує конституційний лад або порушує територіальну цілісність [22].

Порушення закону про медіа може включати різні дії або практики, які суперечать законодавчим нормам, регулюючим галузь медіа. Визначення порушень може залежати від конкретного законодавства країни. Ось деякі загальні види порушень, які можуть виникати в контексті законодавства про медіа: розповсюдження неправдивої інформації або навмисне приховування фактів з метою введення громадськості в оману; невиконання норм та етичних стандартів журналістської етики, таких як недостовірна робота,

конфлікт інтересів тощо; намагання обмежити або придушити свободу преси, наприклад, шляхом запобігання наданню інформації, переслідування журналістів тощо; поширення інформації без перевірки достовірності або використання необ'єктивних джерел; порушення конфіденційності або розсекречування інформації, яка повинна залишатися конфіденційною; використання політичного впливу для впливу на зміст та спосіб висвітлення подій; створення та поширення матеріалів, які можуть призвести до підриву громадського порядку чи загрожувати національній безпеці; зловживання рекламними матеріалами, наприклад, неправдивими обіцянками або подачею інформації як новин.

Потрібно зазначити, що визначення порушень може варіюватися в залежності від конкретного законодавства та правил, що діють у кожній конкретній країні. Громадські та професійні організації часто відіграють роль у визначенні та нагляді за дотриманням етичних та законодавчих стандартів у медіаіндустрії.

В умовах воєнного стану гостро постає питання про необхідність єдиної інформаційної політики. У зв’язку з цим Президент України підписав Указ № 152/2022 про введення в дію рішення Ради національної безпеки і оборони України «Про реалізацію єдиної інформаційної політики в умовах воєнного стану».

«Ураховуючи пряму військову агресію з боку російської федерації, активне поширення державою-агресором дезінформації, викривлення відомостей, а також виправдовування або заперечення збройної агресії російської федерації проти України, з метою донесення правди про війну, забезпечення єдиної інформаційної політики в період дії в Україні правового режиму воєнного стану Рада національної безпеки і оборони України вирішила установити, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об’єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається

переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини #UAразом»» [73].

Удосконалення інформаційної політики України в умовах війни вимагає комплексного та гнучкого підходу. Пропонуємо деякі практичні рекомендації, які можуть допомогти у цьому контексті:

1. Реформування системи підготовки кадрів Державної служби спеціального зв'язку та захисту інформації України [https://cip.gov.ua/ua/news] та Центру кібербезпеки (CERT-UA) [https://cert.gov.ua/about-us], розвиток кадрового потенціалу у сфері інформаційної безпеки та кібербезпеки, відповідальних за розробку та координацію інформаційних заходів та комунікаційної стратегії в умовах війни з наступних питань: криптографічний захист інформації; технічний захист інформації; авторизація безпеки інформації; аналітика оцінки вразливостей; тестування систем захисту інформації.

2. Працювати з демократичними державами для зміцнення стабільності кіберпростору та критичної інфраструктури з урахуванням досвіду відбиття агресії російської федерації проти України в кіберпросторі та ефективно протистояти атакам російських державних установ і хакерів: важливо розвивати партнерства та обмін досвідом між державами для ефективного виявлення, протидії та відновлення внаслідок кібератак; проводити спільні вправи та тренування для підвищення навичок у сфері кібербезпеки та відповіді на кіберзагрози; створити системи для швидкого та безпечного обміну інформацією про кіберзагрози між державами; розвивати спільні стандарти та протоколи у сфері кібербезпеки для забезпечення сумісності та взаємодії між системами; впроваджувати заходи для захисту критичної інфраструктури від кіберзагроз та розробляти плани надзвичайних ситуацій; активно лобіювати та підтримувати розвиток міжнародних стандартів у сфері кібербезпеки; проводити інформаційні кампанії для свідомого громадянства та підвищення рівня обізнаності щодо кіберзагроз; розробляти та

вдосконалювати механізмів реагування на кібератаки, включаючи швидку реакцію та відновлення після інцидентів.

3. Розвиток систем реагування на дезінформацію Центром протидії дезінформації [https://cpd.gov.ua/category/reports/]: встановлення ефективної системи моніторингу та реагування на дезінформацію; підтримка та розвиток фактчекінгових ініціатив для перевірки правдивості інформації та розкриття маніпуляцій; використання спеціалізованих інструментів для моніторингу соцмереж і виявлення поширення дезінформації; проведення інформаційних кампаній для пояснення громадськості небезпек та шкідливості дезінформації. залучення громадськості та міжнародних експертів.

4. Підвищення цифрової грамотності через оновлену Рамку цифрової компетентності громадян Міністерство цифрової трансформації України: запуск освітніх кампаній щодо цифрової грамотності для громадян та працівників в сфері інформаційних технологій.

«Оновлена версія Рамки (DigComp UA 2.2) враховує: новітні технології, які стали загальнодоступними, такі як штучний інтелект (ШІ) на основі машинного навчання (МН), доповнена реальність (AR), віртуальна реальність (VR), вбудовані (embedded) та носимі (wearable) технології, інтернет речей (IoT) тощо; появу нових державних електронних інформаційних ресурсів, реєстрів та послуг; появу нових викликів сьогодення, а саме, пов’язаних із введенням воєнного стану в Україні: різке збільшення кількості внутрішньо переміщених осіб, біженців, громадян, які проживають на тимчасово окупованих територіях, численне збільшення громадян, які змушені працювати та навчатися дистанційно; виклики широкомасштабної інформаційної війни, пропаганди та кіберзагроз з боку країни- агресора, інші виклики сьогодення» [https://osvita.diia.gov.ua/uploads/1/7451-ramka_cifrovoi_kompetentnosti.pdf].

Розвиток цифрових технологій сприяє новим можливостям для зростання національної економіки України та покращення якості життя громадян. Використання цих можливостей є серйозним викликом і важливим

завданням для українського суспільства.

5. Створення медіа організацій для забезпечення прозорості та незалежності медіаорганізацій, відкритості їх власності та джерел фінансування, наприклад:

Hromadske TV (громадське ТБ) [https://hromadske.ua/; https://www.prostir.ua/author/hromadske-tv/] – незалежний медіа-проект, який був створений для забезпечення об'єктивної інформації. Hromadske TV активно прагне до фінансової відкритості та взаємодії з глядачами через різні канали.

Texty.org.ua [https://texty.org.ua/] – медіа-організація, яка спеціалізується на журналістських розслідуваннях та докладному аналізі.

Detector Media [https://detector.media/] – центр медіа-розвідки, який зосереджується на моніторингу медіа-середовища в Україні.

Interfax-Ukraine [https://interfax.com.ua/] - новинне агентство, яке надає новини та інформацію в Україні. Ця організація дотримується журналістських стандартів та прагне до об'єктивності у своїй діяльності. «Інтерфакс-Україна – найбільше інформагентство України. За даними міжнародної дослідницької компанії GfK-Україна, Інтерфакс-Україна є лідером у нашій країні за всіма ключовими показниками роботи серед інформагентств (цитування в ЗМІ, охоплення аудиторії, оцінка бізнес-спільнотою таких категорій, як неупередженість у висвітленні подій, оперативність у наданні інформації тощо). Інтерфакс-Україна є активним членом Європейської Бізнес Асоціації та Американської торговельної палати в Україні».

Ukrayinska Pravda [https://www.pravda.com.ua/rus/] – незалежний новинний портал, який спеціалізується на розслідуваннях та аналітиці. Вони визначають себе як відкритий та прозорий ресурс.

6. Ефективна зовнішня комунікація, що вимагає систематичної роботи, стратегічного підходу та уваги до потреб різних груп зацікавлених сторін:

розвиток стратегій ефективної зовнішньої комунікації для висвітлення ситуації в Україні та залучення підтримки міжнародної громадськості; забезпечення чіткості та зрозумілості усіх комунікаційних повідомлень; сприяння взаємодії з громадськістю та забезпечення механізмів для отримання зворотного зв'язку; використання різноманітних каналів, таких як прес-конференції, соціальні мережі, веб-сайти, електронна пошта для розповсюдження інформації; забезпечення відкритості та доступності інформації для громадськості; чесність та відкритість у відносинах з представниками ЗМІ та громадськістю; встановлення конструктивних відносин із журналістами та надання їм доступу до важливих інформаційних подій; розвиток та підсилення позитивного бренду та іміджу органів публічного управління через ефективну комунікацію; розробка плану реагування на кризові ситуації та його використання для забезпечення ефективної комунікації в умовах негативних подій; визначення цільової аудиторії та адаптація комунікаційних стратегій для різних груп громадськості; організація заходів, таких як круглі столи, конференції, де представники органу публічного управління можуть взаємодіяти з громадськістю та ЗМІ; гнучкість у комунікаційних стратегіях та здатність адаптуватися до змін в інформаційному середовищі.

7. Розробка антидезінформаційних кампаній: проведення антидезінформаційних кампаній для роз'яснення та висвітлення фактів, зменшення впливу дезінформації.

8. Розвиток медійної грамотності: запуск освітніх програм медійної грамотності для розуміння громадянами особливостей роботи медіа та виявлення і розпізнавання дезінформації та розвитку критичного мислення серед громадян; впровадження найкращих світових практик, що спираються на досвід Європейської рамки кваліфікацій та американської Стратегічної освітньої ініціативи у сфері кібербезпеки:

– National initiative for cybersecurity education (NICE) – **і**ніціатива, спрямована на підвищення кібербезпеки в США шляхом розвитку та

підтримки освітніх та професійних програм у галузі кібербезпеки.

– Cybersecurity and infrastructure security agency (CISA) – агентство, яке веде роботу в сфері кібербезпеки та інфраструктурної безпеки в США.

– National initiative for cybersecurity careers and studies (NICCS) - програма, яка забезпечує ресурси та інформацію для розвитку кар'єри в галузі кібербезпеки.

– Federal Virtual Training Environment (FedVTE) - віртуальна платформа для навчання фахівців у сфері кібербезпеки з використанням онлайн-курсів та ресурсів.

– National Centers of Academic Excellence (CAE) - програма, яка визначає та підтримує вищі навчальні заклади, що викладають програми у сфері кібербезпеки, забезпечуючи їх високими стандартами.

9. Ефективна кібербезпека інформаційної інфраструктури від кібератак: зміцнення заходів кібербезпеки для захисту інформаційної інфраструктури від кібератак; проведення регулярних аудитів безпеки та оцінок ризиків для ідентифікації потенційних вразливостей та загроз; розробка та впровадження докладного плану кіберзахисту, який включає в себе заходи протидії, відновлення та навчання персоналу; вимагання від користувачів використовувати складні та унікальні паролі, а також використання двоетапної аутентифікації; встановлення та поновлення програм антивірусного захисту та антималварних засобів для виявлення та блокування шкідливих програм; регулярне встановлення оновлень та патчів для операційних систем, програмного забезпечення та застосунків для усунення вразливостей; застосування мережевих заходів безпеки, таких як файрволи, виявлення вторгнень та безпека мережевого обладнання; впровадження систем моніторингу та аналізу подій для вчасного виявлення та реагування на аномальну діяльність; регулярне створення резервних копій даних та їх зберігання в безпечному місці для відновлення у випадку кібератаки; розгляд можливості отримання страхового покриття від кіберризиків для фінансового захисту в разі інциденту; співпраця з іншими

організаціями, урядовими установами та спеціалізованими службами для обміну інформацією та взаємодопомоги в справі кібербезпеки.

10. Розвиток гібридної війни, де комбінуються різні методи бойових дій, включаючи військові, політичні, економічні, інформаційні та інші, з метою досягнення стратегічних цілей без відкритого зіткнення: розробка стратегій ведення гібридної війни, включаючи використання інформаційних, кібернетичних та психологічних інструментів; розробка онлайн-ресурсів для перевірки фактів та спростування міфів; застосування розрядженої інформації для впливу на громадську думку, дезінформації та маніпуляції інформаційним простором; використання комп'ютерних атак для завдання шкоди критичним інформаційним системам та інфраструктурі; здійснення економічних санкцій, бойкотів та інших заходів для виклику економічної нестабільності; використання дипломатичних засобів для надання або відмови від підтримки в залежності від ситуації; здійснення втручання в політичний процес інших країн, включаючи вплив на вибори та роботу політичних інститутів; використання аспектів енергетичної безпеки для досягнення стратегічних цілей, наприклад, змінюючи ціни на енергоресурси; використання терористичних методів та технік в гібридних операціях; застосування методів соціальної інженерії для маніпуляції особистісними чинниками та груповою динамікою.

Гібридна війна вимагає комплексного та інтегрованого підходу до захисту національної безпеки та виявлення адаптивних стратегій для ефективності в умовах постійної зміни методів та загроз.

11. Залучення громадськості: забезпечення активної участі громадськості у створенні та виконанні інформаційної політики, включаючи підтримку ініціатив та співпрацю з активістами та журналістами.

12. Міжнародна співпраця: взаємодія з міжнародними партнерами для обміну досвідом та отримання підтримки у сфері інформаційної політики.

Таким чином, запропоновані рекомендації можуть допомогти українському уряду створити ефективну та адаптовану до умов війни

інформаційну політику, спрямовану на захист інформаційного простору та підтримку громадян; служити основою для подальших обговорень та розробки конкретних стратегій для зміцнення інформаційної політики в умовах війни в Україні. Удосконалення інформаційної політики України в умовах війни включає широкий спектр заходів, спрямованих на зміцнення внутрішньої та зовнішньої інформаційної безпеки, підвищення свідомості громадян та ефективну комунікацію.

Висновки до другого розділу

Нормативно-правові аспекти у сфері інформаційної політики визначаються законами та іншими нормативно-правовими актами, які регулюють збір, обробку, збереження та використання інформації в органах публічного управління. У багатьох країнах це може включати в себе заходи для забезпечення конфіденційності, доступності, цілісності та безпеки інформації. Україна також має своє законодавство, яке регулює ці аспекти: Закон України «Про інформацію», Закон України «Про доступ до публічної інформації», Закон України «Про захист персональних даних» та додаткові нормативно-правові акти, внутрішні положення та регламенти, що регулюють конкретні аспекти інформаційної політики в конкретних органах чи секторах.

Ці закони та акти спрямовані на забезпечення законності, захисту прав та інтересів громадян та бізнесу в контексті інформаційної взаємодії з державними органами. Важливо відзначити, що законодавство може змінюватися, і рекомендується перевіряти останні зміни в законодавстві для отримання актуальної інформації.

Ефективна інформаційна політика органів публічного управління може суттєво посилити національні зусилля щодо мирного вирішення кризових ситуацій. Навпаки, ігнорування факторів повідомлення, а часто й свідома зміна повідомлення може спровокувати найрадикальніші настрої,

спалахи ворожнечі та призвести до катастрофічних наслідків. Використання інформаційних технологій військовими відкриває нові можливості для забезпечення оборони країни. Володіння інформаційними ресурсами та їх захист у військовій сфері стали такими ж неодмінними атрибутами, як зброя, боєприпаси, транспорт тощо. Перемога України у військово-інформаційному конфлікті з росією сприятиме досягненню її стратегічних цілей. Стратегія інформаційної безпеки України відображає національні інтереси, зокрема необхідність ефективного захисту конституційного ладу національного суверенітету та територіальної цілісності, встановлення та підтримки політичної стабільності, у тому числі стабільності державної влади та її інститутів. Аналіз реалізації стратегічних цілей показує, що, незважаючи на труднощі під час воєнного стану, процес не зупинився.

ВИСНОВКИ

Висновки щодо теоретико-методологічних засад інформаційної політики органів публічного управління можуть бути сформульовані наступним чином:

1. Основною теоретичною засадою є необхідність стратегічного підходу до інформаційної політики органів публічного управління. Це передбачає визначення чітких стратегічних цілей, завдань і пріоритетів у сфері обробки та управління інформацією для досягнення місій та завдань організації.

2. Забезпечення конфіденційності та безпеки інформації є важливими аспектами теоретичних засад. Визначення правил доступу, шифрування даних, заходів кібербезпеки та відповідності стандартам сприяє ефективній захисту конфіденційної інформації.

3. Забезпечення доступності та цілісності інформації покликане гарантувати, що інформація буде доступною для тих, хто має на це право, в той час як буде збережено її непошкоджений стан.

4. Теоретичні засади вказують на важливість інтеграції інформаційних систем та технологій для оптимізації робочих процесів та підвищення ефективності органів публічного управління.

5. Визначення відповідальності та етичних принципів є ключовою теоретичною засадою. Забезпечення етичної поведінки в обробці інформації та розподіл відповідальності між співробітниками сприяє виконанню інформаційної політики.

6. Теоретичні принципи вказують на необхідність адаптації до технологічних змін. Швидка реакція на технологічні інновації та забезпечення їхньої взаємодії з інформаційною політикою дозволяє органам публічного управління залишатися конкурентоспроможними та ефективними.

Довгострокове реформування системи суспільно-політичних відносин в Україні ставить перед науковцями, державними діячами та державними діячами завдання ефективної державної інформаційної політики органів публічного управління як інструменту регулювання взаємодії всіх складових суспільно-політичної системи, насамперед держави, громадянське суспільство та ЗМІ. Її вирішення безпосередньо залежить від соціально-політичного і культурного рівня і зрілості політичної свідомості, а також від адекватності політичної ідеології суспільно-політичному процесу. Події російсько-української війни посилили та прискорили процес розвитку інформаційної політики органів публічного управління. Інформаційна політика органів публічного управління воєнного часу включає комплекс дій і заходів регулятивного, організаційного, контрольного та іншого характеру, спрямованих на дотримання принципу свободи діяльності у сфері ЗМІ та забезпечення балансу суспільних інтересів і інтересів суспільства. Країна перебуває в стані відсічі збройній агресії.

Підсумовуючи, хочеться підкреслити, що підвищення рівня достовірності інформації, максимально ефективне використання інформаційних ресурсів, зовнішніх і внутрішніх інформаційних каналів в умовах війни дозволить підвищити якість управлінських рішень органів влади, політично-соціальної стабільності. Стабільність військової системи, суспільно-політичний розвиток у надзвичайних ситуаціях сприятимуть перемозі на полі бою в Україні

Отже, формування інформаційної безпеки в умовах війни є складною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист країни, суспільства та людини. У воєнний період захист національної інформаційної безпеки є першочерговим завданням, оскільки безпосередньо пов’язаний з безпекою суспільства і людини. Під час війни охорона публічного права виходить за рамки традиційних прав і включає приватноправові відносини. Необхідно розуміти, що держава часто об’єктивно не в змозі повністю захистити права людини. Проте збереження

фундаментальної основи політико-правової взаємодії на основі механізмів інформаційної безпеки може захистити основи демократії та систему єдиних правових принципів від підриву добровільними рішеннями.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Абрамов В.І. Гібридна війна як нова форма міждержавного протиборства: стратегія перемоги. Виклики і загрози національній безпеці в умовах гібридної війни: матеріали наук.-практ. семінару (Київ, 27 квітня 2017 р.) К. : НАДУ, 2017. С. 17-22.

2. Антонюк В. В. Інформаційна війна в структурі сучасного геополітичного протиборства: нові контексти та інтерпретації. *Державне управління: удосконалення та розвиток.* 2021. № 7. URL: http://www.dy.nayka.com.ua/?op=1&z=2121

3. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: монографія; за загальною редакцією д-ра юрид. наук, проф. Бандурки О.М. Харків: Вид-во Ун-ту внутр. Справ, 2000. 368 с.

4. Бабенко Ю. Інформаційна війна – зброя масового знищення. URL.: https://www.pravda.com.ua/rus/articles/2006/04/20/4399050/./

5. Бартош Н.В. Актуальні питання удосконалення реалізації державної інформаційної політики України в умовах гібридної війни. *Публічне урядування*, 3 (28). 2022. С. 17-24. http://journals.maup.com.ua/index.php/public-management/article/view/1290

6. Березовська І.Р. Державна інформаційна політика України та основні напрями її вдосконалення / І.Р. Березовська, Д.М. Русак. *Міжнародні відносини. Серія «Економічні науки».* 2014. № 4. URL: http://journals. iir.kiev.ua/index.php/ec_n/issue/view/132

7. Воронкова В.Г. Технології інформаційного менеджменту в державному управлінні. *Вісник Національного університету цивільного захисту України : зб. наук. пр.* Харків : Вид-во НУЦЗУ, 2021. Вип. 2 (15). 509 с. (Серія "Державне управління"). С.70-79. URL: http://vdu-nuczu.net/ua/8-ukr/141-vipusk-2-15-2021

8. Воронкова В.Г., & Нікітенко В.О. Креативне місто як чинник

розвитку цифрового суспільства. *Комунальне господарство міст*. Харків, 2022. Том 2 № 169 (2022): Серія: Економічні науки. С.57-64. URL: https://khg.kname.edu.ua/index.php/khg/article/view/5935

9. Воронкова В.Г., Васильчук Г.М., Каганов Ю.О., Нікітенко В.О., Метеленко Н.Г. Розробка моделі цифрової освіти у контексті європейської програми DigiComp 2.0. *Humanities studies:* Collection of Scientific Papers / Ed.V. Voronkova. Zaporizhzhia : Publishinghouse "Helvetica", 2023. 15 (92).

10. Воронкова В.Г., Венгер О.М. Формування концепції адміністративного менеджменту в умовах стрімкого розвитку технологій, стохастичності та адаптивності до змін. *Humanities studies : зб. наук. пр. / Запоріз. нац. ун-т.* Запоріжжя: ЗНУ, 2020. №3 . Р. 159-177.

11. Воронкова В.Г., Нікітенко В.О., Васильчук Г.М. Agile-філософія як чинник форсайту цифрової економіки. *Цифрова економіка та економічна безпека*. Одеса: Причорноморський науково-дослідний інститут економіки та інновацій 2022. № 3(03). С. 109-117. URL: https://repository.sspu.edu.ua/handle/123456789/13379?locale=uk

12. Воронкова, Валентина, Кивлюк, Ольга, & Андрюкайтене, Регіна. Еволюція від активного відповідального громадянства до цифрового в контексті критичного мислення: досвід країн ЄС. *Humanities studies: Collection ofScientific* Papers / Ed. V. Voronkova. Zaporizhzhia : Publishinghouse"Helvetica", 2023. 14 (91). P.23–34.

13. Воронкова, Валентина, Нікітенко, Віталіна, & Васильчук Геннадій. Філософія цифрового розвитку креативного міста. *Humanities studies: збірник наукових праць* / гол. ред. В.Г.Воронкова. Запоріжжя : видавничий дім «Гельветика», 2022. Випуск 12 (89). С.16-26

14. Гіда О.Ф. Щодо основних засад формування державної інформаційної політики. *Боротьба з організованою злочинністю (теорія і практика).* 2013. №1 (29). С. 333–341.

15. Голованова Н. В. Інформаційна політика України в умовах війни (архетипний підхід). *Наукові перспективи.* No 6. (24). 2022. URL:

http://perspectives.pp.ua/index.php/np/article/view/1864/1862

16. Горовий В.М. Правові перспективи національного розвитку. URL: http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/nablizhajuchi-derzhavu-do-suspilstva/#st hash.AgJjKJa4.dpuf

17. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12.03.22 р. № 263. URL: https://zakon.rada.gov.ua/ laws/show/263-2022п#Text.

18. Довгань О.Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації. Правова інформатика. 2013. № 4(40). С. 79-88.

19. Дорогих С.О. Щодо питань інформаційної безпеки як напряму інформаційної політики України в умовах війни. Інформація і право. № 2(41)/2022. URL: https://ippi.org.ua/sites/default/files/17_20.pdf

20. Дубов Д.В. Державна інформаційна політика України в умовах гібридного миру та війни. *Стратегічні пріоритети*. 2016. No 3. С. 86–93. URL: http://nbuv.gov.ua/UJRN/spa_2016_3_12.

21. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національногоуніверситету «Львівська політехніка». Серія: Юридичні науки*. 2020. Т. 7. №2. С. 56–61.

22. Закон України «Про медіа». URL: https://zakon.rada.gov.ua/laws/show/2849-20#n2350

23. Закон України «Про державну таємницю». Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

24. Закон України «Про доступ до публічної інформації». Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

25. Закон України «Про захист персональних даних». Відомості

Верховної Ради України (ВВР), 2010, № 34, ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Tex

26. Закон України «Про науково-технічну інформацію». Відомості Верховної Ради України (ВВР), 1993, № 33, ст.345. URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text

27. Закону України «Про інформацію». Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

28. Заніздра Н.О. Державна інформаційна політика на сучасному етапі та шляхи вдосконалення. *Вісник КрНУ імені Михайла Остроградського.* 2012. №4. С. 193–196.

29. Захаренко К. Проблеми формування ефективної державної інформаційної політики. *Філософія.* Випуск 36(49), 2016. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/18225/Zaharenko.pdf?sequence=1

30. Звіт про врахування пропозицій, які надійшли за результатами обговорень в рамках підготовки плану дій із впровадження Ініціативи «Партнерство «Відкритий Уряд» у 2023-2025 роках. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/partnerstvo/zvit-ogp-2023-2025_propos.pdf

31. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни: навч. посіб. Том 1. НЛП XX століття. 2-е видання, виправлене та доповнене. К.: Вид-во «Люта справа», 2015. 384 с.

32. Зозуля О. С. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства: дис. … канд. наук з держ. упр.: спец. 25.00.01. / НАДУ. Київ, 2017. 261 с.

33. Іванченко Ю.М. Сутність, головні напрями та способи державної інформаційної політики в Україні. *Державне управління: теорія та практика.* 2005. № 2. URL: http://www.academy.gov.ua/ej/ej2/

34. Інформаційна політика в Україні: конспект лекцій. / Укладачі В.О. Шведун, Т.О. Луценко. Х.: НУЦЗУ, 2016. 40 с. URL: http://nnvc.nuczu.edu.ua/images/topmenu/kafedry/kafedra-publichnoho-administruvannia-u-sferi-tsyvilnoho-zakhystu/Lekcii/lk5.pdf

35. Кабінет Міністрів України – Презентовано Центр стратегічних комунікацій та інформаційної безпеки. Головна / Кабінет Міністрів України. URL: https://www.kmu.gov.ua/news/prezentovano-centr-strategichnihkomunikacij-ta-informacijnoyi-bezpeki.

36. Картки: що таке стратегічна комунікація і кому вона потрібна. URL: https://cpc.com.ua/ articles/kartki-scho-take-strategichna-komunikaciya-ikomu-vona-potribna.

37. Концепція розвитку електронного урядування в Україні. Схвалено розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text

38. Косогоров О., Сірик А. Основні проблемні питання та напрями підвищення ефективності державної інформаційної політики України в умовах гібридної війни. Інформаційний вимір гібридної війни: досвід України : матеріали міжнародної науково-практичної конференції. Київ: НУОУ, 2017. С. 44–46. URL: https://nuou.org.ua/assets/documents/zbirn-gibr-mizhn-konf.pdf

39. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції.* № 1. 2022. URL: http://apnl.dnu.in.ua/1_2022/25.pdf

40. Красноступ Г.М. Основні напрями правового забезпечення державної інформаційної політики. Офіційний веб-сайт Міністерства юстиції України. URL: http://old.minjust.gov.ua/30768

41. Марутян Р. Інформаційний складник гібридної війни проти України: сучасні виклики та загрози. URL: https://matrix-info.com.

42. Марченко О. В. Правові засади державної інформаційної політики.

Прикарпатський юридичний вісник. Випуск 3(9) том 2, 2015. URL: http://www.pjv.nuoua.od.ua/v3-2_2015/30.pdf

43. Мельник М. Сутність поняття «державна політика розвитку інформаційного суспільства»: узагальнення європейських та вітчизняних трактувань. *Науковий вісник «Демократичне врядування».* 2012. Вип. 9 URL: http://www.lvivacademy.com/vidavnitstvo_1/visnik9/ fail/Melnyk.pdf

44. Мороз Н. С. Державна інформаційна політика України у сфері інформатизації діяльності органів державної влади. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4867/moroz1.pdf

45. Національний інформаційний простір України: проблеми формування та державного регулювання *Аналітична доповідь. Національний інститут стратегічних досліджень.* Київ. 2013. URL: https://niss.gov.ua/sites/default/files/2013-11/1119_dop.pdf

46. Негодченко В. Основні напрями державної інформаційної політики в Україні. *Інформаційне право*. 4/2016. URL: http://www.pgp-journal.kiev.ua/archive/2016/04/15.pdf

47. Нестеряк Ю.В. Нормативно-правові основи державної інформаційної політики України в умовах розвитку інформаційного суспільства. *Теорія та практика державного управління*. 2012. Вип. 4(39). С. 111–119.

48. Осьодло В.І., Будагьянц Л.М. Соціально-філософські та психологічні аспекти сучасних війн: монографія. К.: Видавничий дім «ЕртЕк», 2018. 408 с.

49. Офіційний веб-сайт міжнародної Ініціативи «Партнерство «Відкритий Уряд»: URL: https://www.opengovpartnership.org/

50. Пахнін М.Л. Принципи, завдання та інструменти державної інформаційної політики України в сучасних умовах. *Теорія та практика державного управління.* Вип. 3(46). С.1–9.

51. Підвищення рівня цифрової грамотності українців: Мінцифри презентує оновлену Рамку цифрової компетентності громадян.

https://www.kmu.gov.ua/news/pidvyshchennia-rivnia-tsyfrovoi-hramotnosti-ukraintsiv-mintsyfry-prezentuie-onovlenu-ramku-tsyfrovoi-kompetentnosti-hromadian

52. План дій із впровадження Ініціативи «Партнерство «Відкритий Уряд у 2021-2022 роках», затверджено розпорядженням Кабінету Міністрів України від 24 лютого 2021 р. № 149-р. URL: https://zakon.rada.gov.ua/laws/show/149-2021-%D1%80#Text

53. Пожуєв В.І. Формування державної інформаційної політики в умовах глобалізації. *Гуманітарний вісник Запорізької державної інженерної академії.* 2010. Вип. 43. С. 4–12.

54. Почепцов Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття. К.: Видавничий дім «Києво-Могилянська академія», 2017. 260 с.

55. Почепцов Г. Смисли і війни : Україна і Росія в інформаційній і смисловій війнах. К.: Видавничий дім «Києво-Могилянська академія», 2016. 316 с.

56. Почепцов Г. Сучасні інформаційні війни. Вид. 3-є. доповн. та переробл. К.: Видавничий дім «Києво-Могилянська академія», 2016. 504 с.

57. Про нейтралізацію загроз інформаційній безпеці держави: Рішення Ради національної безпеки і оборони від 18.03.22 р. URL: https://zakon.rada.gov.ua/laws/show/n0003525-22#n2

58. Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану: Наказ Головнокомандувача Збройних Сил України від 03 березня 2022 року №73. URL:https://www.mil.gov.ua/content/mou_orders/nakaz_73_050322.pdf?fbclid=IwAR3BFiXuFblkYZgRCWVYGHffTJhtmhBbQXAEVE7KZ-MR00Q_i6gzSslnkFg. /.

59. Проект Плану відновлення України. Матеріали робочої групи «Діджиталізація». Національна рада з відновлення України від наслідків

війни. 2022. https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/digitization.pdf

60. Пунда О.О., Добрянська О.Д., Новицька Н.Б. Принципи інформаційної політики в умовах війни та їх нормативно-правове закріплення. *Екологічне право*. 2022. №1-2. С. 60–65.

61. Рамка цифрової компетентності громадян України. DigCompUA for Citizens 2.2. 2023. URL: https://osvita.diia.gov.ua/uploads/1/7451-ramka_cifrovoi_kompetentnosti.pdf

62. Результати діяльності Центру протидії дезінформації РНБО України за 2023 рік. URL: https://cpd.gov.ua/main/rezultaty-czentru-protydiyi-dezinformacziyi-rnbo-ukrayiny-za-2023-rik/

63. Розпорядження Кабінету міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні» від 20 вересня 2017 р. № 649-р. URL: https://www.kmu.gov.ua/npas/250287124

64. Сайт Центру протидії дезінформації РНБО України. URL: https://cpd.gov.ua/category/events/

65. Самотуга А. Значення програмних документів держави у законодавчому забезпеченні проактивної зовнішньої інформаційної політики України. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2021. № 4. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2022/02/NV4/%D0%9C%D0%B0%D0%BA%D0%B5%D1%82_%D0%9D%D0%92_4-2021_%D0%BC%D1%8F%D0%B3%D0%BA-99-109.pdf

66. Світова гібридна війна: український фронт / За заг. ред. В.П. Горбуліна. Національний інститут стратегічних досліджень. Київ : НІСД, 2017. 496 с.

67. Селезньова О. Теоретико-методологічні основи інформаційного права України: моногр. / О. Селезньова. Чернівці: Місто, 2014. 408 с.

68. Соснін О.В. Державна інформаційна політика і національні інформаційні ресурси. URL: http://old. niss.gov.ua/book/D_p2.htm

69. Сутність та головні напрями державної інформаційної політики України / Мохова Ю.Л., Луцька А.І. *Державне управління: удосконалення та розвиток*. 2018 р. No 12.

70. Терещенко В.В. Особливості державної інформаційної політики в умовах війни. *Юридичний науковий електронний журнал.* URL: http://www.lsej.org.ua/2_2023/92.pdf

71. Токар О. Державна інформаційна політика: проблеми визначення концепту. *Політичний менеджер*. 2009. № 5. С.131–141.

72. Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

73. Указ Президента України №152/2022 Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». URL: https://www.president.gov.ua/documents/1522022-41761

74. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12

75. Череп А., Воронкова В., Череп О. Цифрова трансформація суспільства як необхідна умова його інноваційного розвитку. *Теорія і практика інтелектуальної власності.* 2022. №2. С. 68-72. URL: http://uran.inprojournal.org/article/view/259745

76. Чукут С.А., Джига Т.В. Інформаційна політика в Україні (опорний конспект лекцій до нормативного курсу): Навчальний посібник. К.: 2007. 94 с. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/Opornij-konspekt-lektsij_CHukut_Dzhiga_Informatsijna-politika-v-Ukrayini.pdf

77. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану: Рішення Ради національної безпеки і оборони від 19.03.22 р. URL: https://zakon.rada.gov.ua/laws/show/n00045 25-22#Text

78. Federal Virtual Training Environment. URL:

https://fedvte.usalearning.gov/

79. National Centers of Academic Excellence. URL: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

80. National Cybersecurity Strategy. March 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

81. National initiative for cybersecurity careers and studies (NICCS). URL: https://niccs.cisa.gov/

82. National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. URL: https://www.cisa.gov/national-initiative-cybersecurity-education-nice-cybersecurity-workforce-framework