

**Міністерство освіти і науки України
Дніпровський державний аграрно-економічний університет
Факультет менеджменту і маркетингу
Кафедра менеджменту, публічного управління та адміністрування**

**ДОПУСТИТИ ДО ЗАХИСТУ
В ЕКЗАМЕНАЦІЙНІЙ КОМІСІЇ:**

**Завідувачка кафедри,
д.держ.упр., проф.
_____ Наталія БОНДАРЧУК
« ____ » _____ 2024 р.**

КВАЛІФІКАЦІЙНА РОБОТА

**на тему: УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ
ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ ВОЄННОГО СТАНУ**

Освітньо-професійна програма «Публічне управління та адміністрування»
Спеціальність 281 «Публічне управління та адміністрування»
Ступінь вищої освіти: Магістр

Здобувач

Василь СТАДНИК

**Науковий керівник,
д.держ.упр., проф.**

Наталія БОНДАРЧУК

Дніпро – 2024

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ АГРАРНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ**Факультет:** Менеджменту і маркетингу**Кафедра:** Менеджменту, публічного управління та адміністрування**Освітньо-професійна програма:** «Публічне управління та адміністрування»**Спеціальність:** 281 «Публічне управління та адміністрування»**Ступінь вищої освіти:** Магістр

ЗАТВЕРДЖУЮ

Зав. кафедри _____

« ____ » _____ 202_р.

ЗАВДАННЯ**на підготовку кваліфікаційної роботи****Стадника Василя Григоровича**

(прізвище, ім'я, по батькові)

1. Тема роботи: «Удосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану»**Науковий керівник:** Бондарчук Н.В., д. держ. упр., проф.,

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по ДДАЕУ від « ____ » _____ 202_ року № _____

2. Термін подання здобувачем роботи: 4 грудня 2024 року _____**3. Вихідні дані до роботи:** Закони України, Постанови КМУ, Накази Міністерства освіти і науки, Укази Президента України та інші нормативні документи, навчальні посібники, підручники, періодична література, праці провідних вчених з публічного управління та адміністрування.**4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)**1. Теоретичні засади інформаційного забезпечення органів державної влади. Аналіз стану інформаційного забезпечення органів державної влади в умовах воєнного стану. Напрями вдосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану. Висновки та пропозиції.**5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)**Властивості, які належать інформації. Підходи до визначення поняття «інформаційне забезпечення». Ключові рівні якості використання інформаційних систем в органах державної влади. Завдання комунікаційних підрозділів в органах державної влади.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____ 11 жовтня 2023 р. _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Затвердження теми кваліфікаційної роботи	жовтень 20223р.	
2.	Пошук та опрацювання літературних джерел	листопад-грудень 2023р.	
3.	Написання Розділу 1. «Теоретичні зачати інформаційного забезпечення органів держаної влади»	січень - березень 2024р.	
4.	Написання Розділу 2. «Аналіз стану інформаційного забезпечення органів державної влади»	квітень - травень 2024р.	
5.	Написання Розділу 3. «Напрями вдосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану»	червень - листопад 2024р.	
6	Написання загальних висновків	грудень 2024р.	
7	Оформлення роботи	грудень 2024р.	

Здобувачка _____
(підпис)

Василь СТАДНИК
(прізвище та ініціали)

Науковий керівник _____

Наталія БОНДАРЧУК

РЕФЕРАТ

Тема: «Удосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану»

Кваліфікаційна робота містить: 78 с., 8 рис., 4 табл., 54 літературне джерело.

Об'єкт дослідження - процес інформаційного забезпечення органів державної влади в умовах воєнного стану.

Предмет дослідження теоретико-методичні та прикладні аспекти щодо удосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану.

Метою роботи полягає у дослідженні теоретичних та розробці практичних рекомендацій щодо удосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану.

Методи дослідження методи синтезу, аналізу, індукції, дедукції, графічний, стратегічний.

Проаналізовано зміст поняття «інформаційне забезпечення» в державному управлінні. Досліджено особливості інформаційного забезпечення в умовах кризових ситуацій. Проаналізовано стан нормативно-правового регулювання інформаційного забезпечення в умовах воєнного стану. Досліджено основні проблеми та недоліки інформаційного забезпечення органів державної влади в умовах воєнного стану. Надано пропозиції щодо удосконалення інформаційного забезпечення в умовах воєнного стану. Практичні рекомендації щодо удосконалення інформаційного забезпечення органів державної влади запропоновано впроваджувати в діяльність Підгородненської міської ради Дніпровського району Дніпропетровської області.

КЛЮЧОВІ СЛОВА

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ, ОРГАНИ ДЕРЖАВНОЇ ВЛАДИ, ВОЄННИЙ СТАН, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРЗАГРОЗА

KEYWORDS

INFORMATION SECURITY, GOVERNMENT BODIES, MARTIAL LAW, INFORMATION SECURITY, CYBER THREAT

ЗМІСТ

ВСТУП	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ	9
1.1. Сутність і значення інформаційного забезпечення в державному управлінні	9
1.2. Особливості інформаційного забезпечення органів державної влади в умовах кризових ситуацій	17
1.3. Методологічні основи аналізу ефективності інформаційного забезпечення органів державної влади	19
Висновки до розділу 1	28
РОЗДІЛ 2. АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ ВОЄННОГО СТАНУ	30
2.1. Нормативно-правове регулювання інформаційного забезпечення органів державної влади в умовах воєнного стану	30
2.2. Стан інформаційного забезпечення Підгородненської міської ради	33
2.3. Виявлення основних проблем і недоліків інформаційного забезпечення Підгородненської міської ради в умовах воєнного стану	38
Висновки до розділу 2	41
РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ ВОЄННОГО СТАНУ	43
3.1. Іноземний досвід інформаційного забезпечення органів державної влади	43
3.2. Забезпечення кібербезпеки та захисту інформаційних потоків органів державної влади	47
3.3. Рекомендації щодо посилення комунікації між державними органами і громадянами в умовах воєнного стану	53
Висновки до розділу 3	65
ВИСНОВКИ	67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	71

ВСТУП

Актуальність теми дослідження. В умовах воєнного стану інформаційне забезпечення органів державної влади набуває особливої важливості, оскільки саме через ефективну комунікацію та управління інформаційними потоками можливо забезпечити оперативність, точність і надійність прийняття управлінських рішень. Воєнний стан характеризується високим рівнем нестабільності, швидкою зміною ситуацій і постійними загрозами, що вимагає підвищеної уваги до організації інформаційних процесів.

Ефективне інформаційне забезпечення є запорукою координації між різними органами влади, забезпечення належної взаємодії з військовими структурами, громадськістю та міжнародними партнерами. Зокрема, це стосується розповсюдження достовірної інформації, попередження дезінформації та забезпечення прозорості дій влади, що є важливим для підтримки довіри громадян і стабільності в суспільстві.

Наразі існує потреба у вдосконаленні інформаційної інфраструктури, впровадженні сучасних цифрових технологій, створенні захищених каналів комунікації та забезпеченні інформаційної безпеки. Ці аспекти стають критично важливими для реагування на кризові ситуації, збереження державної цілісності та захисту національних інтересів.

Питаннями інформаційного забезпечення займалися багато дослідників, які розглядали цей аспект із різних наукових і практичних точок зору. Так, Вінер Н. розглядав інформацію як ключовий елемент адаптації системи до зовнішнього середовища, що заклало основи для розуміння інформації як ресурсу. Акофф Р. акцентував увагу на упорядкованій інформації, яка використовується для прийняття управлінських рішень. Нонака І. досліджував інформаційні потоки та знання як базу для управління та навчання організацій. Він підкреслював, що інформація є основою ефективного прийняття рішень. Коломієць Є. вивчала інформацію як знання,

що інтегруються в комунікаційні процеси, об'єднуючи технічні та соціальні аспекти. Синеокий О. та Кормича Б. досліджували правові та організаційні аспекти інформаційного забезпечення. Їхні роботи спрямовані на аналіз нормативно-правової бази, яка регулює інформаційну діяльність

Дослідження та впровадження ефективних механізмів інформаційного забезпечення органів державної влади в умовах воєнного стану є не лише актуальним, а й необхідним для забезпечення національної безпеки та ефективного державного управління.

Мета та завдання дослідження. Мета дослідження полягає у дослідженні теоретичних та розробці практичних рекомендацій щодо удосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану.

Для реалізації поставленої мети в роботі окреслено наступні завдання:

- проаналізувати зміст поняття «інформаційне забезпечення» в державному управлінні;
- дослідити особливості інформаційного забезпечення в умовах кризових ситуацій та методологічні основи аналізу ефективності;
- проаналізувати стан нормативно-правового регулювання інформаційного забезпечення в умовах воєнного стану;
- виявити основні проблеми і недоліки інформаційного забезпечення органів державної влади в умовах воєнного стану;
- дослідити іноземний досвід інформаційного забезпечення органів державної влади;
- надати пропозиції щодо удосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану.

Об'єктом дослідження є процес інформаційного забезпечення органів державної влади в умовах воєнного стану.

Предметом дослідження є теоретико-методичні та прикладні аспекти щодо удосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану.

Методи дослідження. В ході написання кваліфікаційної роботи використано загальнонаукові методи, такі як аналіз і синтез, індукція та дедукція, а також порівняльний аналіз для вивчення міжнародного досвіду інформаційного забезпечення органів державної влади. Крім того, застосовано емпіричний метод для збору та аналізу конкретної інформації щодо інформаційного забезпечення органів державної влади в умовах воєнного стану.

Інформаційну базу дослідження становлять законодавчі та нормативно-правові акти, що регулюють роботу органів державного управління та місцевого самоврядування, наукові дослідження, аналітичні звіти, статистичні дані, а також досвід інших країн, які мали справу з аналогічними викликами

Наукова новизна дослідження полягає у наданні практичний рекомендацій щодо удосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану. Основні положення, що мають елементи новизни, полягають у такому:

удосконалено

- комплексний план дій, спрямований на захист інформаційних систем державних органів від кібератак, зокрема в умовах воєнного стану.

- інструменти підвищення ефективної комунікації між державними органами та громадянами в умовах воєнного стану, які враховують сучасні цифрові технології, забезпечення зворотного зв'язку та підвищення довіри до органів влади;

набуло подальшого розвитку

- способи імплементації зарубіжного досвіду інформаційного забезпечення органів державної влади в Україні;

Апробація результатів роботи. Результати проведеного дослідження обговорювалися на науково-практичних конференціях: III міжнародній науково-практичній Інтернет-конференції «Актуальні проблеми економіки, управління та маркетингу в аграрному бізнесі» (м. Дніпро, 03-04 жовтня

2024р); XII-й науково-практичній Інтернет - конференції «Розвиток форм і методів сучасного менеджменту в умовах глобалізації» (м. Дніпро 8-9 листопада 2024 р). За результатами досліджень опубліковано статтю у Міжнародному науковому журналі «Інтернаука» (категорія Б).

Кваліфікаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел, що нараховує 54 найменування, містить 8 рисунків, 4 таблиці. Основний зміст кваліфікаційної роботи магістра викладено на 77 сторінках друкованого тексту.

РОЗДІЛ 1.

ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

1.1. Сутність і значення інформаційного забезпечення в державному управлінні

Інформаційне забезпечення є однією з ключових складових ефективного функціонування системи державного управління. Воно охоплює процеси збору, обробки, аналізу, зберігання та передачі інформації, необхідної для прийняття управлінських рішень. У сучасному суспільстві інформація виступає стратегічним ресурсом, який безпосередньо впливає на якість управління, швидкість реагування на виклики та рівень довіри громадян до державних інституцій.

Сутність інформаційного забезпечення полягає у створенні умов для ефективної комунікації та обміну інформацією між органами державної влади, а також між державою та громадянами. Це забезпечення включає не лише технічні аспекти, такі як інфраструктура та програмні засоби, але й організаційні, правові та кадрові компоненти. Таким чином, інформаційне забезпечення є системним явищем, що охоплює всі рівні державного управління.

Якість і швидкість інформаційного забезпечення значно впливають на ефективність будь-яких управлінських процесів. У загальному сенсі, інформаційне забезпечення є системою показників та засобів їх опису, таких як класифікатори, коди, економічна документація та інформаційні бази.

Інформація, в свою чергу, визначається як дані про стан системи чи навколишнього середовища, які сприймаються людиною або спеціальним пристроєм. Інформація, яка потрібна для оптимальної роботи управлінської системи, називається управлінською [7].

Інформація, як інструмент організації управління соціальними системами, є найбільш ефективним засобом з точки зору державного управління. В управлінні соціальними системами інформацію можна визначити як задокументовані або публічно озвучені дані про події та явища, що відбуваються у суспільстві, державі чи природному середовищі, які використовуються для здійснення управлінської діяльності. Сучасна наука, досліджуючи роль інформації у публічному управлінні, розробила низку підходів, що висвітлюють різні аспекти цього феномену [12].

Практичний аспект розуміння інформації, що тісно пов'язаний як із антропоцентричним підходом, так і з підходом, заснованим на понятті "дані", висвітлений у дослідженнях Б. Кормича [12]. Вона визначає інформацію як знання (дані), які безпосередньо інтегровані в комунікативний процес.

Варто зазначити, що в законодавстві України поняття інформації залишається неоднозначним і потребує чіткого визначення.

Таблиця 1.1

Сучасні підходи до трактування поняття «інформація»

Автор/джерело	Зміст поняття
міжнародний стандарт ISO/IEC 5127:2001 [49]	Знання, яке стосується певних об'єктів, наприклад, фактів, подій, речей, процесів чи ідей, включаючи концепції, яке в межах певного контексту має конкретний зміст.
стандарт ISO/IEC 10746–2:2009 [50]	Будь-який вид знань, якими можуть обмінюватися користувачі, про речі, факти, поняття і так далі, у всесвіті дискурсу.
О. В. Синеокий [37]	Відомості щодо людей, предметів, фактів, подій, явищ і процесів, незалежно від форми їх подання, передані усним, письмовим або іншим способом, в тому числі за допомогою умовних сигналів, технічних засобів.
Б. А. Кормич [12]	Відомості, що були організовані в такій формі, документовані, передані або оголошені таким чином, що можуть бути сприйнятими іншою особою.
англійський бізнес-словник [48]	Факти, точні дані, які організовані в певному порядку для досягнення певної мети, які подані в контексті що пояснює їх значення.
Закон України «Про інформацію» [25], та в Цивільному кодексі України	Будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Потреба в управлінській інформації у менеджерів є специфічною формою

ставлення до певної інформації, яка визнається необхідною для вирішення конкретних завдань. Основними факторами, що впливають на формування інформаційних потреб менеджерів, є характер управлінської діяльності та особливості функцій, які вони виконують. Ці потреби також залежать від рівня управління, на якому працює менеджер, і від специфіки його завдань у системі господарської діяльності.

Аналіз аспектів розгляду інформації та її ролі у публічному управлінні дозволяє глибше розкрити властивості цього поняття та відобразити їх у більш повному обсязі (рис. 1.1).

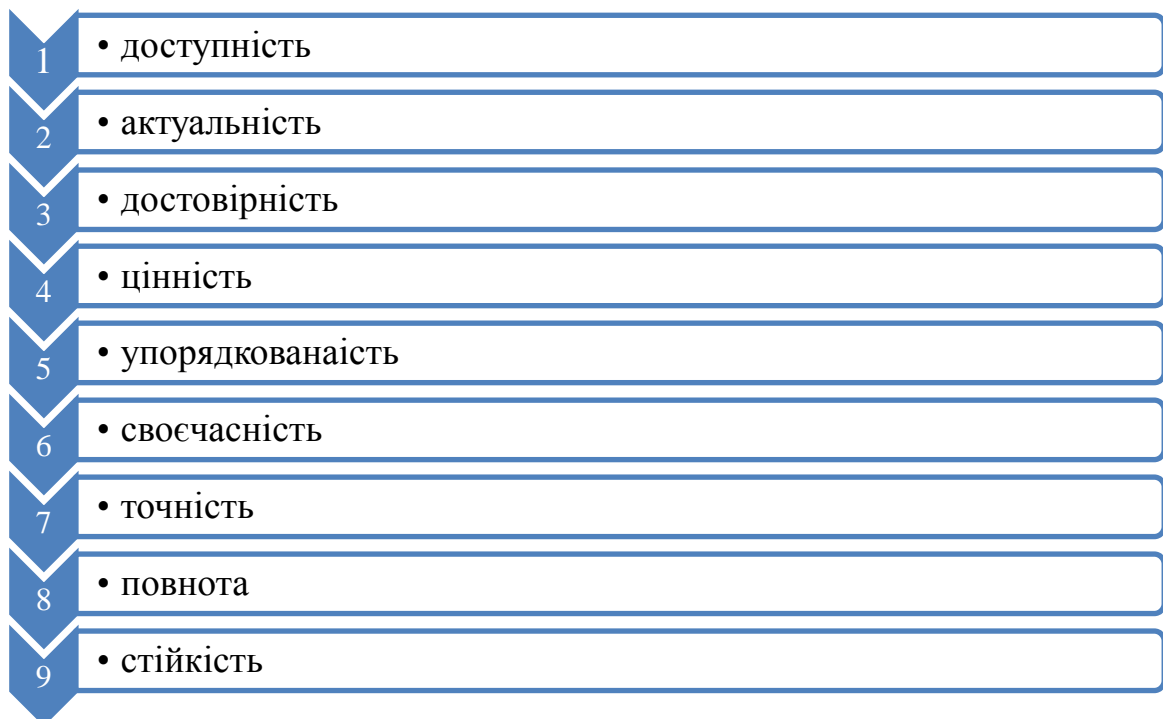


Рис. 1.1. Властивості, які належать інформації

Інформація, як ключовий ресурс у публічному управлінні, демонструє багатовимірні характеристики, що визначають її значення у процесах прийняття рішень, організації комунікації та управлінської діяльності. Вивчення цих властивостей дає змогу підвищити ефективність її використання та забезпечити якісне управління в суспільстві.

Факторами, що сприяють активізації інформаційної діяльності, є з одного боку створення сотень електронних баз даних, які містять

різноманітну інформацію, а з іншого боку – впровадження та вдосконалення ефективних методів обробки цієї інформації. Однак процес інформаційної роботи ускладнюється низкою об'єктивних чинників. До таких труднощів належать наступні.

- Неповнота та неточність інформації, з якою працюють органи влади. Це може бути пов'язано з браком ресурсів для збору даних, недостатньою взаємодією між державними установами та законодавчими обмеженнями щодо доступу до інформації.

- Обмеженість часу на прийняття рішень. Незалежно від складності проблеми чи обсягу інформації, час на ухвалення публічно-управлінських рішень часто є недостатнім.

- Багатокритеріальність у процесі ухвалення рішень. Органи влади на всіх рівнях мають враховувати численні критерії, що ускладнює процес прийняття ефективних рішень.

- Недостатня культура роботи з інформаційно-аналітичними матеріалами. Це стосується як підготовки, так і використання аналітичних документів, які забезпечують діяльність органів влади [19].

У таких умовах інформаційне забезпечення публічного управління потребує інтерактивного підходу, який дозволяє мінімізувати перелічені обмеження. Як зазначає Кисельов В, інтерактивність створює передумови для запровадження такого явища, як електронна демократія. Це включає можливість кожного громадянина брати участь у формуванні та реалізації державної політики, а також у прийнятті рішень органами влади за допомогою інформаційно-комунікаційних технологій, які забезпечують двосторонній інтерактивний зв'язок між державою, громадянами [7].

Інформаційне забезпечення є однією з ключових складових у публічному управлінні, бізнесі, науці та інших сферах діяльності. Його значення постійно зростає в умовах цифрової трансформації суспільства та глобалізації інформаційних потоків. У різних наукових джерелах термін розглядається з багатьох точок зору.

Виділимо основні підходи до визначення поняття «інформаційне забезпечення».

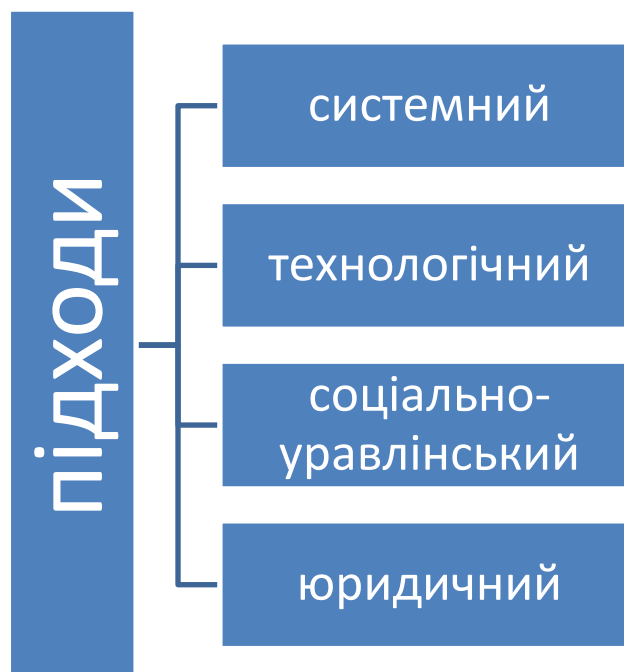


Рис. 1.2. Підходи до визначення поняття «інформаційне забезпечення»

Розвиток поняття «інформаційне забезпечення» відбувався паралельно з прогресом інформаційних технологій. У ранніх дослідженнях акцент робився на класичних інформаційних системах, таких як картотеки та архіви. З часом, внаслідок активного розвитку ІКТ, інформаційне забезпечення почало включати сучасні платформи, бази даних, аналітичні інструменти та засоби кіберзахисту.

У класичних працях Норберта Вінера інформація визначається як зміст, отриманий із зовнішнього середовища, що впливає на процес адаптації системи. Цей підхід розглядає інформацію як основу для функціонування системи, де інформаційне забезпечення виконує роль організаційного ресурсу [52].

За Р. Акоффом, інформаційне забезпечення — це упорядкована та структурована інформація, що використовується для прийняття рішень.

За Є. Коломієць, інформаційне забезпечення — це система збирання, обробки, збереження й поширення даних, яка ґрунтується на використанні сучасних інформаційно-комунікаційних технологій (ІКТ) [7].

Важливу увагу в сучасних дослідженнях приділяється електронним системам документообігу, базам даних та аналітичним платформам, які забезпечують швидкість і точність передачі даних.

На думку українських дослідників, таких як Кисельов В, інформаційне забезпечення є основою для реалізації електронної демократії, яка передбачає інтерактивний зв'язок між органами влади та громадянами [7].

За І. Нонака, інформаційне забезпечення включає потоки повідомлень, які формують основу для прийняття управлінських рішень.

Закон України «Про інформацію» визначає інформаційне забезпечення як діяльність із створення, збору, обробки, зберігання й поширення інформації для задоволення інформаційних потреб громадян, організацій та держави [25].

Інші нормативно-правові акти, такі як закони «Про доступ до публічної інформації» та «Про захист інформації в інформаційно-телекомунікаційних системах», підкреслюють важливість безпеки та доступності інформації в процесах управління [28].

Важливість забезпечення інформацією в державному управлінні зумовлена кількома факторами, серед яких наступні.

1. Прийняття обґрунтованих управлінських рішень. Інформація є основою для аналізу ситуації, прогнозування наслідків і вибору оптимального варіанту дій. Без якісного інформаційного забезпечення державні органи ризикують ухвалювати рішення, які не відповідають реальним потребам суспільства.

2. Забезпечення прозорості та підзвітності. Інформаційне забезпечення дозволяє створити механізми прозорого управління, що підвищує довіру громадян до органів влади. Відкритість інформації про діяльність держави сприяє її підзвітності та ефективності.

3. Оперативність реагування на кризові ситуації. В умовах надзвичайних обставин, таких як природні катастрофи чи воєнний стан, якісне інформаційне забезпечення дозволяє швидко збирати дані, аналізувати їх і приймати своєчасні рішення.

4. Підтримка комунікації з громадянами. Система інформаційного забезпечення сприяє встановленню діалогу між державою та суспільством. Це важливо для інформування населення про державні політики, роз'яснення рішень і мобілізації підтримки в кризових умовах.

У сучасних умовах розвитку цифрових технологій значення інформаційного забезпечення суттєво зросло. Впровадження електронного урядування, цифрових платформ і автоматизованих систем дозволяє оптимізувати управлінські процеси, зменшувати адміністративні витрати та забезпечувати доступність державних послуг.

Однак, інформаційне забезпечення в державному управлінні стикається і з викликами. Це, зокрема, потреба в захисті даних від кібератак, запобігання поширенню дезінформації та забезпечення рівного доступу до інформації для всіх категорій населення. Для подолання цих проблем важливо розробляти та впроваджувати ефективні нормативно-правові акти, інвестувати в технічну інфраструктуру, а також підвищувати рівень кваліфікації працівників, відповідальних за інформаційне забезпечення.

До основних функцій інформаційного забезпечення публічного управління можна віднести такі:

- інформаційна функція – передбачає організацію обміну даними, визначення джерел інформації та способів доступу до них, управління інформаційними потоками, впровадження сучасних технічних засобів і технологій для створення єдиного інформаційного простору;
- управлінська функція – охоплює інформаційний супровід усіх етапів управлінського процесу, включаючи підготовку, прийняття та контроль виконання управлінських рішень;

- інструментальна функція – спрямована на підвищення ефективності публічного управління за рахунок використання інформаційно-комунікаційних технологій (ІКТ) і методів аналізу даних.
- діагностична функція – забезпечує отримання достовірної та об'єктивної інформації про поточну ситуацію, а також організацію зворотного зв'язку;
- прогностична функція – спрямована на виявлення проблем, загроз і потенційних конфліктів для їх своєчасного запобігання;
- пізнавально-ментальна функція – сприяє зміні розуміння явищ, трансформації мислення та ментальності керівників;
- безпекова функція – включає захист інформації від витоку, несанкціонованого доступу, спотворення чи втрати, а також усунення наслідків таких ситуацій [16].

У практичній діяльності найбільш значущими є функції моніторингу ситуації та запитів, експертно-аналітичного забезпечення, збору та первинної обробки даних, створення автоматизованих систем підтримки аналітичних досліджень і надання адміністративних послуг.

Отже, інформаційне забезпечення є багатограним поняттям, яке об'єднує різні аспекти управління, технологій та права. Сучасні дослідження підкреслюють необхідність інтеграції інформаційних технологій для забезпечення прозорості, ефективності та доступності в усіх сферах діяльності. Інформаційне забезпечення публічного управління можна розглядати як специфічний вид діяльності, що здійснюється інформаційними підрозділами органів влади з використанням сучасних інформаційно-комунікаційних технологій. Ця діяльність включає збір, обробку та аналіз даних для прийняття державних управлінських рішень і надання адміністративних послуг.

1.2. Особливості інформаційного забезпечення органів державної влади в умовах кризових ситуацій

В умовах кризових ситуацій, таких як природні катастрофи, економічні потрясіння чи воєнний стан, інформаційне забезпечення органів державної влади стає надзвичайно важливим. Його завдання полягає в забезпеченні ефективного управління, швидкого прийняття рішень та координації дій на всіх рівнях. Від того, наскільки правильно організовано роботу з інформацією, залежить здатність держави оперативно реагувати на виклики, уникати хаосу та забезпечувати безпеку громадян.

Однією з ключових особливостей інформаційного забезпечення в кризових умовах є оперативність. У такі моменти необхідно швидко збирати та обробляти великі обсяги даних. Сучасні технології, такі як моніторингові системи, бази даних та аналітичні платформи, допомагають у цьому процесі. Однак не менш важливою є точність цієї інформації, адже будь-які помилки можуть мати серйозні наслідки, від погіршення ситуації до втрати довіри громадян.

Ще одним викликом у кризових умовах є забезпечення безпеки інформації. Ризик кібератак зростає, тому органи влади мають захищати свої дані від можливих зламів чи втрат. Для цього застосовуються сучасні методи шифрування, створюються резервні копії даних, а також обмежується доступ до конфіденційної інформації.

Кризові ситуації також вимагають ефективної координації між різними відомствами: військовими, поліцією, органами місцевого самоврядування та громадськими організаціями. Для цього створюються спеціальні платформи, де всі учасники можуть обмінюватися актуальною інформацією в реальному часі. Це дозволяє уникнути плутанини та узгодити дії між різними структурами.

Не менш важливою є робота з населенням. У кризових умовах громадяни потребують чіткої інформації про те, що відбувається, як діяти та

які заходи вживаються для їхньої безпеки. Влада повинна активно інформувати людей через засоби масової інформації, соціальні мережі, мобільні додатки або інші канали зв'язку. Важливо, щоб інформація була зрозумілою, своєчасною і правдивою, аби уникнути паніки чи поширення чуток.

Окремо варто виділити протидію дезінформації. У кризових ситуаціях завжди існує ризик поширення неправдивих новин, які можуть використовуватися для дестабілізації ситуації. Тому органи влади мають оперативно реагувати на такі загрози, спростовувати фейки та забезпечувати прозорість своєї діяльності.

Формування теоретико-методологічної основи ідеології інформаційної політики в умовах війни має базуватися на сучасних уявленнях про державну інформаційну політику як систему ідей, цілей, методів і засобів. Ця система дозволяє державі через свої органи і посадових осіб регулювати відносини між громадянським суспільством та інформаційною інфраструктурою держави, яка має значний вплив на суспільні процеси.

Засоби масової інформації орієнтовані на потреби особистості як суб'єкта споживання інформації, забезпечуючи йому доступ до важливих даних. Це сприяє свідомій участі громадян у суспільних змінах та впливу на соціальну практику. У відповідь держава повинна створити нормативно-правову базу, яка буде відповідати актуальним соціальним умовам і забезпечувати ефективну реалізацію інформаційної політики.

Ця база має регулювати як взаємодію держави із засобами масової інформації, так і їхню співпрацю з громадянським суспільством. Основним принципом такої політики є забезпечення доступу до інформації, а також захист державних інтересів від можливих зловживань з боку приватних медіа, що досягається завдяки законодавчому регулюванню.

Інформаційна політика в умовах війни представляє собою комплекс заходів, які реалізуються державою у співпраці з інститутами громадянського суспільства. Ця політика спрямована на регулювання інформаційних

процесів, сприяння формуванню і розвитку інформаційного суспільства, а також захист національних інтересів, особливо у сфері оборони. Основною її метою є забезпечення прав і інтересів людини, підтримка моральних цінностей, а також гарантування інформаційної безпеки особистості, суспільства та держави [14].

Ефективність соціальної системи напряму залежить від ступеня взаємодії та узгодженості між органами державного управління і медіа, які забезпечують двосторонній зв'язок між громадянами та державою. Війна і агресивна інформаційна політика з боку супротивника мають на меті створення атмосфери нестабільності, провокування занепокоєння щодо соціально-економічної ситуації, а також стимулювання деструктивних політико-ідеологічних впливів. Це становить серйозну загрозу для системи національних цінностей, ідеалів і традицій, руйнує соціальні структури, що впливають на особистість, і створює загрози безпеці як на індивідуальному, так і на державному рівні.

1.3. Методологічні основи аналізу ефективності інформаційного забезпечення органів державної влади

Інформація є фундаментальною основою для ухвалення рішень, адже вона визначає напрямки дій, формує послідовність етапів процесу та служить «сировиною», яка піддається збору, обробці та аналізу. Її джерела можуть бути різноманітними: це як загальні знання, так і персональний чи експертний досвід, що часто стають рушіями для прийняття важливих та різноманітних рішень.

Проте існують значні виклики, пов'язані з використанням інформації. По-перше, доступ до необхідної інформації часто обмежений, що може стати перешкодою для прийняття обґрунтованих рішень. По-друге, спеціалізована інформація, яка є ключовим фактором у певних сферах, нерідко

концентрується в руках експертів і може бути важко контролюваною через специфіку доступу або обмеженість ресурсів.

Ці виклики породжують два важливі питання: хто володіє потрібною інформацією та як ця інформація інтерпретується? Умови ієрархічної структури, як у межах одного відомства, так і на рівні всієї держави, роблять ці питання ще більш актуальними. Адже різні рівні доступу до інформації, її суб'єктивна інтерпретація чи обмежений обіг можуть впливати на якість та швидкість ухвалення управлінських рішень.

Окремі документи та масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах) розглядаються як інформаційні ресурси. Інформація, що циркулює в органах державного управління, різноманітна та різноманітна. Вона може відноситися до зовнішньополітичної, економічної, соціально-політичної та екологічної обстановки.

Інформація є ключовим ресурсом для ухвалення управлінських рішень на всіх рівнях - від державного до місцевого. Вона служить основою для розробки нормативних документів і рішень у межах компетенції відповідних органів. Особливу увагу приділяють якісному змісту інформації та кількісній її достатності, адже ці аспекти безпосередньо впливають на ефективність інформаційного забезпечення державного управління [13].

Процес обігу інформації в органах державного управління включає кілька етапів: пошук, збір, обробку, накопичення, зберігання, розповсюдження та споживання. Усі ці операції спрямовані на забезпечення органів державного та муніципального управління якісною інформацією. Якісна інформація має такі ознаки:

- достовірність – інформація повинна бути точною та вільною від помилок.
- сучасність – базується на актуальних даних і відображає поточний стан справ.

- комплексність – охоплює весь спектр питань, пов'язаних із проблемою.
- стислість – подана у зрозумілому, але не перевантаженому вигляді.
- відносність – має безпосереднє відношення до конкретної проблеми [17].

Моніторинг є важливим елементом інформаційного процесу. Отримана в його ході інформація аналізується, оцінюється як самими органами управління, так і вищими державними структурами. На основі аналізу інформації ухвалюються важливі заходи, які можуть включати уточнення цілей і завдань, зміну функцій органів управління, перерозподіл ресурсів або зміну нормативних актів.

Для вирішення будь-якої проблеми інформація повинна бути не лише достовірною, але й значущою. Вона структурується в блоки, які відображають різні аспекти або можливі варіанти вирішення. Цей підхід допомагає виявляти основні причини невирішеності проблеми та пропонувати обґрунтовані шляхи її розв'язання.

У процесі ухвалення державних рішень першорядного значення набуває збір, аналіз і правильне використання повної та достовірної інформації. Зміст такої інформації дозволяє оцінити економічну, соціальну та політичну ситуацію в країні. Інформація збирається спеціалізованими структурами, які відповідають за її повноту та якість, і передається органам, що приймають рішення. Таким чином, інформація стає основою для ефективного управління на всіх рівнях державної влади.

В Україні забезпечення доступу громадян до інформації про діяльність органів державної влади та місцевого самоврядування регулюється Законом України «Про доступ до публічної інформації», який було прийнято у 2011 році. Цей закон спрямований на створення умов для прозорості та відкритості влади, а також надання громадянам можливості отримувати необхідну інформацію про діяльність державних установ [34].

Закон гарантує кожному громадянину право на доступ до інформації, яка знаходиться у розпорядженні державних органів або органів місцевого самоврядування. Інформація, що є відкритою, охоплює такі аспекти, як ухвалені рішення, фінансові звіти, плани роботи, інформація про витрати бюджетних коштів, кадрові призначення тощо. Водночас є обмеження, які стосуються інформації, що становить державну, комерційну чи іншу захищену законом таємницю.

Державні органи зобов'язані забезпечувати регулярне оприлюднення основної інформації через офіційні веб-сайти та інші публічні канали. Громадяни мають право звертатися із запитом до органів влади для отримання додаткової інформації. Такі запити можуть бути подані в електронній або письмовій формі, а органи влади повинні надати відповідь у встановлений законом термін.

Закон також зобов'язує органи влади створювати умови для спрощення доступу до інформації. Це включає використання сучасних цифрових технологій, наприклад, порталу «Дія», який дозволяє громадянам отримувати державні послуги он-лайн.

В даний час використання інформаційних технологій лягло в основу пріоритетної політики, яка отримала назву «електронне держава». З розвитком інформаційних технологій змінюються підходи до організації роботи державні органи. Так, за останні десятиліття суттєво зросло інформаційне навантаження на органи державної влади.

Методологічні основи аналізу ефективності інформаційного забезпечення органів державної влади базуються на комплексному підході до оцінки використання інформаційних ресурсів у процесах управління. Це означає, що аналіз охоплює всі аспекти функціонування інформаційних систем, їхній взаємозв'язок із загальною діяльністю органів влади та здатність сприяти досягненню управлінських цілей.

Перш за все, аналіз інформаційного забезпечення органів влади базується на системному підході. Інформаційні ресурси розглядаються не

ізолювано, а як частина цілісної системи управління. Важливо оцінювати, як ефективність обміну інформацією між підрозділами, доступ до баз даних та їхня інтеграція впливають на швидкість і якість прийняття рішень.

Ще одним ключовим принципом є орієнтація на результативність. Це передбачає оцінку того, наскільки інформаційне забезпечення сприяє досягненню конкретних цілей органів влади, таких як швидке реагування на запити громадян, якість надання адміністративних послуг чи ефективність реалізації державних програм. Аналіз має визначити, чи відповідає обсяг і якість інформації потребам управління.

Важливим аспектом методології є використання кількісних і якісних критеріїв оцінки. Кількісні показники включають, наприклад, швидкість обробки даних, кількість оброблених запитів, доступність інформаційних систем тощо. Якісні критерії стосуються точності, актуальності та зручності інформації для користувачів.

Також враховується адаптивність інформаційних систем до змін у зовнішньому середовищі. У сучасних умовах органи влади повинні бути готові до швидкої адаптації своїх інформаційних ресурсів до нових викликів, таких як воєнний стан, кризи чи технологічні зміни. Це вимагає аналізу стійкості інформаційного забезпечення та його готовності до кіберзагроз.

Методологія включає і принцип орієнтації на громадян. Оцінка ефективності повинна враховувати, наскільки інформаційне забезпечення відповідає потребам населення, чи забезпечує воно прозорість діяльності органів влади та доступ громадян до інформації.

Отже, методологічні основи аналізу ефективності інформаційного забезпечення органів державної влади є багатограними. Вони охоплюють оцінку як технічних аспектів роботи інформаційних систем, так і їхнього впливу на досягнення цілей управління, адаптивності до змін і задоволення потреб громадян. Цей підхід дозволяє системно оцінити ефективність та визначити напрями вдосконалення інформаційного забезпечення.

Інформаційні системи є невід'ємною складовою сучасного інформаційного забезпечення органів державної влади, адже вони виступають ключовим інструментом для забезпечення ефективності управління та прийняття рішень. У швидко змінюваному світі, де обсяги інформації постійно зростають, традиційні підходи до її обробки та використання стають недостатніми. Інформаційні системи дозволяють долати ці обмеження та забезпечувати органам влади сучасні можливості для виконання своїх функцій.

Однією з головних причин важливості інформаційних систем для органів державної влади є їх здатність забезпечувати оперативний доступ до актуальної та достовірної інформації. Це критично важливо для прийняття зважених управлінських рішень, адже без точної інформації керівники ризикують зробити помилки, які можуть мати серйозні наслідки.

Крім того, інформаційні системи сприяють автоматизації рутинних процесів, таких як документообіг, реєстрація звернень громадян, облік ресурсів тощо. Це дозволяє знизити навантаження на працівників, скоротити час на виконання завдань та мінімізувати ймовірність помилок, які часто виникають під час ручної роботи.

Ще одним важливим аспектом є можливість покращення прозорості та підзвітності державних органів. Інформаційні системи дозволяють громадянам отримувати доступ до відкритих даних, контролювати витрати бюджету, відстежувати виконання державних програм та взаємодіяти з органами влади у зручному форматі. Це підвищує довіру до державних інституцій і сприяє формуванню прозорого суспільства.

Розробка інформаційної системи (ІС) для організації є складним процесом, що вимагає дотримання певних стандартів, правил та рекомендацій. Попри труднощі, такі вимоги виправдані, оскільки вони сприяють ефективності та відповідності системи потребам організації. Основні принципи, якими має керуватися розробка ІС, включають:

1. Інформаційна система повинна підвищувати функціональні можливості організації та сприяти її ефективності.
2. Інформаційна структура органів державної влади має динамічно враховувати сучасні досягнення науки та практики управління.
3. Інформаційні ресурси повинні бути прозорими для громадян, але водночас забезпечувати інформаційну безпеку та конфіденційність, відповідати законам і захищати права власності на інформацію.
4. Інформаційна структура повинна відповідати організаційній структурі установи та підвищувати ефективність документообігу.

Одна з головних проблем керівництва державних установ полягає в недостатньому усвідомленні важливості інформаційних технологій та їхніх переваг. Складні інформаційні системи зазвичай розробляються фахівцями разом із залученими консультантами. Однак для того, щоб система була ефективною, у процес розробки необхідно залучати керівників, які надалі будуть користуватися цією системою.

Аналіз інформаційної системи не може обмежуватися лише економічними аспектами діяльності. Процесний підхід до аналізу є найбільш доцільним, оскільки він дозволяє оцінити всі процеси, включно з інформаційними, і знайти шляхи їхньої оптимізації. Першим кроком у розробці ІС має стати аналіз існуючих процесів, їхня переоцінка та планування нової моделі організації. Це включає впровадження підходів до загального управління якістю (TQM), що допомагають раціоналізувати бізнес-процеси та підвищити їх ефективність.

Другим кроком є впровадження самої інформаційної системи після оптимізації всіх процесів. Головною метою цього етапу є забезпечення точності та ефективності інформаційних процесів, які впливають на ухвалення та контроль управлінських рішень. Організації потрібна система, яка дозволяє збирати й зберігати дані, відстежувати ключові показники продуктивності, ідентифікувати проблеми та забезпечувати доступ до

стратегічної інформації. Такий підхід дозволяє значно оптимізувати діяльність і сприяє досягненню кращих результатів.

Моніторинг інформаційної системи організації можна здійснювати за допомогою кількісного аналізу, який дозволяє оцінити її ефективність і відповідність потребам організації. Такий аналіз включає оцінку обсягу вхідної інформації, швидкість її використання або перенаправлення, якщо обробка цієї інформації не входить до обов'язків співробітників організації. Важливим аспектом також є аналіз змісту вхідної інформації: її релевантність, структурованість і узагальненість.

Заключним етапом моніторингу є досягнення максимальної відповідності між впровадженою інформаційною системою та організаційною структурою органу управління. Це означає, що організаційна структура повинна бути гнучкою та адаптованою до нових технологій, а не залишатися статичною. Досягнення такої відповідності передбачає переоцінку використовуваних ресурсів, включно з трудовими, та оптимізацію співвідношення персоналу до експлуатованої інформаційної системи. Організаційна структура має розглядатися як динамічний процес, що постійно змінюється й удосконалюється, а не як фіксована форма.

Одним із найбільш ефективних способів модернізації організаційної структури є реінжиніринг бізнес-процесів. Цей підхід передбачає аналіз, спрощення та реконструкцію існуючих процесів з використанням сучасних інформаційних технологій. Реінжиніринг дозволяє оптимізувати робочі процеси, усунути дублювання завдань і значно підвищити продуктивність, а також якість продуктів і послуг. Це методика, яка передбачає новий підхід до організації роботи та є більш ефективною, ніж традиційна раціоналізація.

Основна ідея підходу до впровадження та використання інформаційних систем (ІС) в органах державного управління полягає у поступовому досягненні трьох стадій «зрілості»: якості інформації, якості процесів та якості організаційної структури

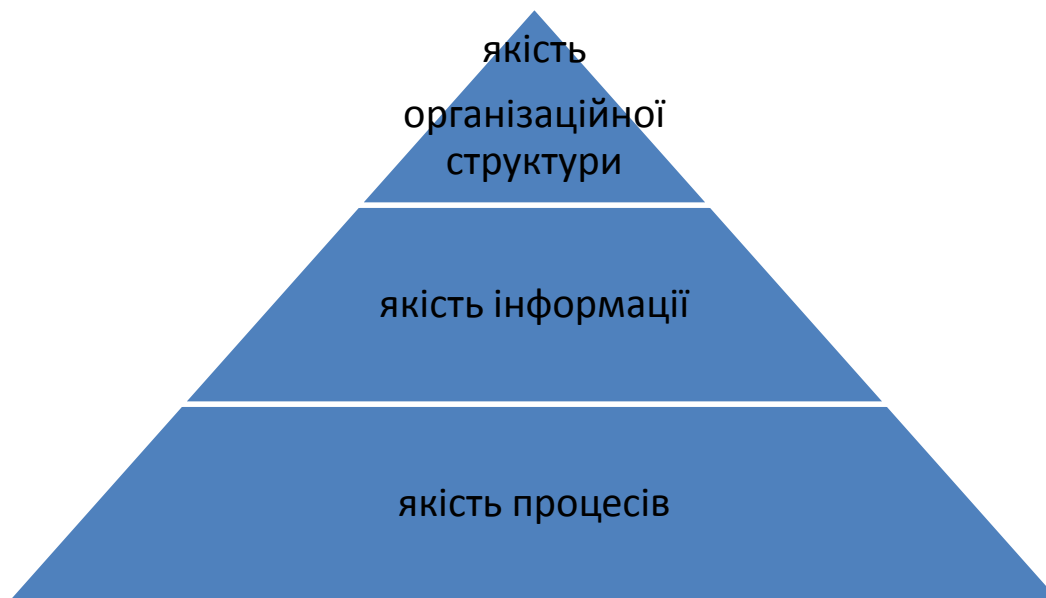


Рис. 1.3. Ключові рівні якості використання інформаційних систем в органах державної влади

Ці стадії формують основу для систематизації та підвищення ефективності інформаційних процесів. Лише після досягнення третього рівня, який забезпечує повну організаційну ефективність, система стає стабільно дієвою та приносить максимальні вигоди.

Необхідність у такій поступовій структурі пояснюється тим, що неефективність у будь-якій із цих сфер створює ланцюгову реакцію. Наприклад, неефективна організація процесів і управління інформаційними потоками призводить до неефективності всієї організаційної структури. У результаті, якщо організація не досягає рівня зрілості у своїй діяльності, переваги від впровадження ІС будуть мінімальними або взагалі непомітними.

ІС, яка проходить всі три стадії зрілості та впроваджується послідовно, забезпечує стійку роботу організації до тих пір, поки зовнішні чи внутрішні обставини не викличуть потребу в її оновленні. Наприклад, збільшення кількості завдань, зростання обсягу процесів чи вплив непередбачених обставин можуть вимагати перегляду існуючих підходів до роботи. Крім того, використання застарілих технологій та інновацій, у тому числі

інформаційно-комунікаційних технологій (ІКТ), може знижувати ефективність роботи. У таких випадках стає необхідною переоцінка процесів, функціональності ІС та рівня кваліфікації персоналу.

Таким чином, успішне впровадження та використання ІС залежить від постійної адаптації до нових умов, що передбачає регулярний перегляд і вдосконалення процесів та технологій, забезпечуючи організаціям стабільний розвиток та гнучкість у реагуванні на зміни.

Висновки до розділу 1

1. Інформаційне забезпечення є критично важливим елементом державного управління, оскільки воно забезпечує ефективність прийняття рішень, прозорість діяльності органів влади та оперативність реагування на виклики. У сучасному суспільстві інформація є стратегічним ресурсом, який впливає на управлінські процеси та рівень довіри громадян до державних інституцій. Інформаційне забезпечення вимагає інтеграції технічних, організаційних, правових і кадрових аспектів для досягнення ефективності управління.

2. В умовах кризових ситуацій (наприклад, війни чи катастроф) інформаційне забезпечення стає основою для швидкого та точного ухвалення рішень. Воно забезпечує оперативний збір, аналіз і передачу даних, сприяє координації між відомствами, інформуванню населення та протидії дезінформації. Важливими аспектами є забезпечення точності, безпеки даних і використання сучасних технологій для досягнення максимальної ефективності в управлінні.

3. Ефективність інформаційного забезпечення органів влади залежить від комплексного підходу до його оцінки, який враховує технічні, організаційні та соціальні аспекти. Ключовими є системність аналізу, орієнтація на досягнення результатів, використання кількісних і якісних показників, а також адаптивність до змін. Інформаційні системи є важливим

інструментом для оптимізації управлінських процесів, автоматизації рутинних завдань і забезпечення прозорості діяльності органів влади. Ефективна розробка та впровадження ІС в органах державної влади потребує поступового досягнення трьох стадій: якості інформації, якості процесів та якості організаційної структури. Лише після досягнення цих рівнів зрілості ІС може забезпечувати стабільну та ефективну роботу організації. Важливими етапами є аналіз існуючих процесів, їх оптимізація, впровадження сучасних технологій і регулярна переоцінка системи для адаптації до змін.

РОЗДІЛ 2

АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ ВОЄННОГО СТАНУ

2.1. Нормативно-правове регулювання інформаційного забезпечення органів державної влади в умовах воєнного стану

В умовах воєнного стану забезпечення якісною інформацією державного управління набуває особливого значення, адже оперативний і надійний обмін інформацією стає критично важливим для прийняття ефективних управлінських рішень, збереження національної безпеки та стабільного функціонування органів влади. В цей період інформаційна діяльність органів державної влади та місцевого самоврядування регулюється не лише загальними нормативно-правовими актами, а й спеціальними правовими інструментами, які враховують специфіку надзвичайного становища.

В умовах воєнного стану в Україні забезпечення якісною інформацією органів державної влади регулюється низкою нормативно-правових актів, які визначають порядок доступу до інформації, її захист та особливості функціонування інформаційних систем. Основним документом, що встановлює правовий режим воєнного стану, є Закон України «Про правовий режим воєнного стану» [33]. Цей закон визначає зміст воєнного стану, порядок його введення та скасування, а також повноваження органів державної влади в цих умовах.

З метою забезпечення інформаційної безпеки та протидії інформаційним загрозам, Президент України затвердив Стратегію інформаційної безпеки. Цей документ окреслює актуальні виклики в інформаційній сфері та визначає стратегічні цілі для захисту національних інтересів [42].

Питання регулювання державної інформаційної політики в умовах війни та воєнного стану визначені у низці законодавчих актів, зокрема в указах Президента України. Серед них указ від 24 лютого 2022 року №64/2022 «Про введення воєнного стану в Україні», а також указ «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року щодо реалізації єдиної інформаційної політики в умовах воєнного стану».

В даних указах запроваджено правовий режим воєнного стану, визначено заходи, необхідні для захисту країни, і встановлює особливі умови функціонування державних органів, у тому числі в сфері інформаційного забезпечення, надано повноваження для обмеження або регулювання доступу до певної інформації, якщо це необхідно для забезпечення безпеки та громадського порядку.

Указ «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [26]. Цей указ спрямований на координацію діяльності органів державної влади в інформаційній сфері. У ньому підкреслюється важливість забезпечення єдиної інформаційної політики, яка включає:

- узгоджену комунікацію державних органів з громадянами та міжнародною спільнотою;
- протидію дезінформації та інформаційним впливам з боку агресора;
- захист інформаційного простору країни від зовнішніх загроз;
- формування позитивного інформаційного порядку денного та консолідацію суспільства.

Основою правового регулювання залишаються такі ключові закони: Конституція України, Закон України «Про правовий режим воєнного стану», «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних» та інші акти, які визначають загальні принципи

інформаційної діяльності. Однак в умовах воєнного стану додаються додаткові механізми для забезпечення безпеки інформаційних потоків.

Закон України «Про інформацію» визначає основи відносин, пов'язаних зі створенням, збором, зберіганням, використанням та поширенням інформації. Основними напрямками державної інформаційної політики, за цим законом, є забезпечення доступу до інформації для кожного, розвиток інформаційного суспільства, створення умов для прозорості діяльності органів влади, впровадження електронного урядування та забезпечення інформаційної безпеки [25].

Закон «Про Національну програму інформатизації» окреслює загальні засади створення і реалізації цієї програми, яка покликана вирішувати проблеми інформаційного забезпечення у соціально-економічній, екологічній, оборонній та інших сферах загальнодержавного значення. Ця програма охоплює концепцію, державні та галузеві проекти, а також ініціативи органів місцевого самоврядування [29].

Закон «Про електронні документи та електронний документообіг» регулює порядок створення, передачі, зберігання та обробки електронних документів. Він визначає правові основи їх використання органами державної влади та місцевого самоврядування, а також підприємствами та організаціями всіх форм власності.

Закони «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про захист персональних даних» регулюють питання захисту інформації, включаючи державні інформаційні ресурси та персональні дані. Вони встановлюють вимоги до безпеки інформації та правил її обробки.

Під час воєнного стану вводяться додаткові механізми для забезпечення безпеки інформаційних потоків. Наприклад, важливо захистити інформацію, пов'язану з військовими діями, щоб запобігти її використанню ворогом. Також посилюються заходи кіберзахисту, адже кібератаки стають серйозною загрозою для державних систем.

Доступ до публічної інформації в умовах воєнного стану може бути обмежений. Це необхідно для захисту національної безпеки. Наприклад, деякі дані можуть бути недоступними для громадськості, щоб уникнути їх використання ворожими силами.

Органи місцевого самоврядування теж повинні швидко адаптуватися до умов. Вони мають оперативно інформувати населення про надзвичайні події, евакуацію чи гуманітарну допомогу. Для цього часто використовуються електронні платформи, які дозволяють швидше передавати інформацію.

Втім, існують проблеми. На місцях не завжди достатньо розвинені інформаційні системи, а електронний документообіг часто функціонує лише частково. Крім того, різні бази даних державних органів не завжди інтегровані між собою, що ускладнює обмін інформацією.

Важливою частиною роботи з інформацією є її захист. Держава зобов'язана забезпечити збереження персональних даних громадян, особливо вразливих категорій, таких як внутрішньо переміщені особи чи військові.

Підсумовуючи, забезпечення якісною інформацією органів державної влади в умовах воєнного стану є складним, але критично важливим завданням. Для цього потрібні сучасні технології, кіберзахист і чітке дотримання законодавства, щоб гарантувати ефективну роботу держави та безпеку її громадян.

2.2. Стан інформаційного забезпечення Підгородненської міської ради

Підгородненська міська територіальна громада була офіційно створена 27 вересня 2019 року внаслідок об'єднання п'яти населених пунктів Дніпровського району Дніпропетровської області. До складу громади увійшли місто Підгородне, яке стало її адміністративним центром, а також села Перемога, Спаське, Хуторо-Губиниха та Дмитрівка. Ця адміністративно-

територіальна реформа стала важливим кроком для консолідації ресурсів, підвищення ефективності управління та покращення рівня життя мешканців громади.

Загальна площа Підгородненської територіальної громади становить 225,51 кв. км, а її населення складає 21 648 мешканців станом на 6 серпня 2024 року. Громада активно розвиває комунікацію з мешканцями та місцевими підприємцями, впроваджуючи сучасні підходи до інформування та взаємодії. Значну роль у цьому відіграють офіційні сторінки громади в соціальних мережах, які слугують основними каналами для поширення актуальної інформації, анонсів, новин, а також для оперативного реагування на запити та пропозиції громадян.



Рис. 2.1. Офіційні сторінки громади в соціальних мережах

Підгородненська міська рада активно використовує сучасні інформаційні технології для забезпечення прозорості своєї діяльності та ефективної комунікації з мешканцями громади. Основним інструментом є офіційний веб-сайт ради, де розміщуються новини, оголошення, рішення ради та виконавчого комітету, а також інша важлива інформація для громадян.

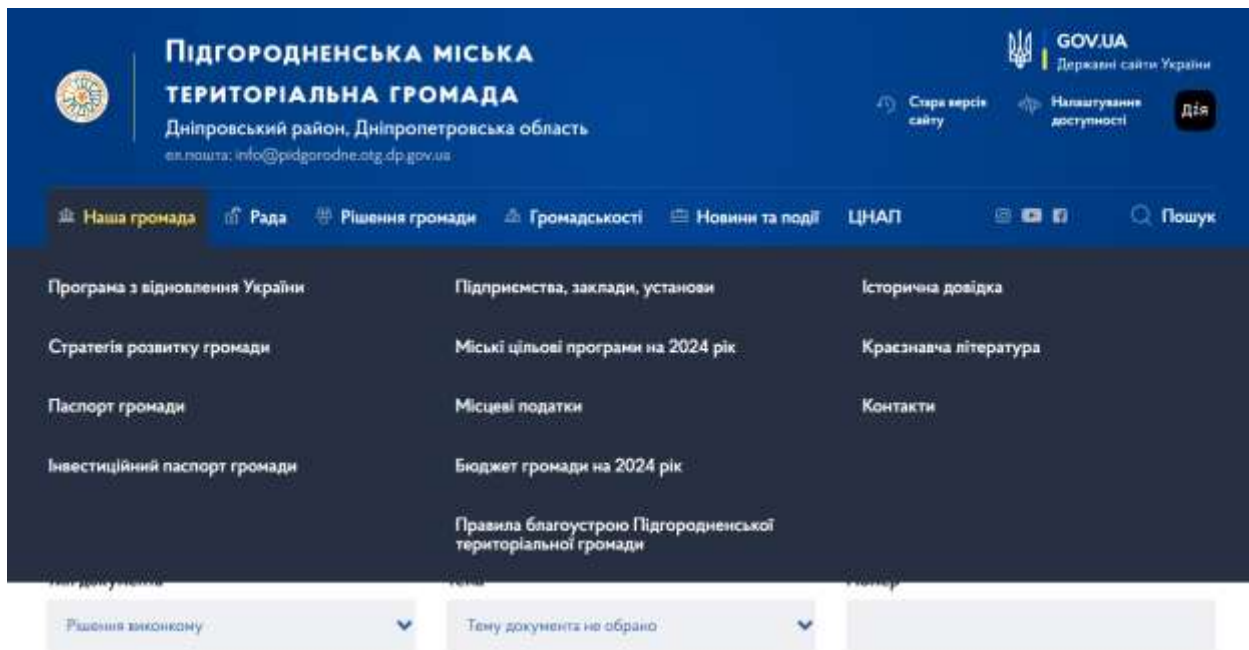


Рис. 2.2. Офіційний веб-сайт Підгородненської міської ради

На веб-сайті розміщуються актуальні новини, що висвітлюють основні події у громаді, рішення виконавчого комітету та міської ради, що стосуються різних аспектів життя громади, включаючи соціальну підтримку, інфраструктурні проекти, бюджетні рішення та адміністративні послуги. Оголошення на сайті дають змогу громадянам своєчасно отримувати інформацію про заплановані заходи, громадські слухання, терміни подання документів та інші важливі події.

Важливим розділом веб-сайту є публікація документів, таких як протоколи засідань ради, плани розвитку громади, фінансові звіти та рішення щодо використання бюджетних коштів. Це забезпечує доступ громадян до детальної інформації про діяльність влади, сприяючи підвищенню довіри до органів самоврядування.

Окрім цього, веб-сайт містить інтерактивні форми для подачі запитів та звернень громадян. Це дозволяє мешканцям безпосередньо взаємодіяти з органами влади, висловлювати свої пропозиції, скарги чи отримувати консультації. Усе це сприяє формуванню відкритого діалогу між владою та громадою.

Крім офіційного веб-сайту, Підгородненська міська рада активно використовує соціальні мережі, зокрема Facebook, як один із ключових інструментів комунікації з мешканцями громади. Офіційна сторінка ради у Facebook регулярно оновлюється, що дозволяє оперативно донести до громадян важливу інформацію, новини та оголошення.

Через соціальні мережі міська рада інформує мешканців про актуальні події, такі як громадські слухання, зустрічі з представниками влади, культурні та спортивні заходи, а також про нові проєкти чи ініціативи, що реалізуються в громаді. Це сприяє підвищенню поінформованості громадян та їхньої залученості до життя громади.

Однією з ключових переваг соціальних мереж є можливість швидкого реагування на нагальні ситуації. Наприклад, через Facebook громада може бути оперативно проінформована про надзвичайні ситуації, зміни в роботі комунальних служб, перекриття доріг чи інші важливі питання.

Також соціальні мережі створюють простір для двосторонньої комунікації. Мешканці мають можливість коментувати публікації, ставити запитання чи надсилати пропозиції безпосередньо через сторінку ради. Це забезпечує зворотний зв'язок, який є важливим для оцінки потреб і очікувань громадян.

Крім того, активність у соціальних мережах дозволяє охопити ширшу аудиторію, включаючи молодь та інші категорії населення, які рідше використовують традиційні засоби комунікації. Соціальні мережі стають не лише платформою для поширення інформації, але й інструментом для зміцнення довіри між владою та громадою.

Завдяки використанню соціальних мереж, таких як Facebook, Підгородненська міська рада демонструє сучасний підхід до взаємодії з громадянами, забезпечуючи прозорість своєї діяльності та залучаючи мешканців до участі у вирішенні питань місцевого значення.

Центр надання адміністративних послуг (ЦНАП) Підгородненської міської ради є важливою складовою системи обслуговування населення,

спрямованою на спрощення доступу до державних і місцевих адміністративних послуг. ЦНАП працює для того, щоб забезпечити зручність, прозорість і швидкість у вирішенні питань, які виникають у мешканців громади.

Через ЦНАП надається широкий спектр послуг, зокрема:

- реєстрація місця проживання та зняття з реєстрації. Мешканці громади можуть оформити або змінити реєстрацію свого місця проживання без зайвих складнощів. Ця послуга є однією з найбільш затребуваних і забезпечується у максимально стислі терміни;
- видача різних видів довідок. Наприклад, довідок про склад сім'ї, підтвердження проживання на території громади, довідок для отримання соціальної допомоги тощо. Це дозволяє громадянам оперативного отримати необхідні документи для подальшого використання;
- надання соціальних послуг. ЦНАП виступає посередником між мешканцями та органами соціального захисту, допомагаючи оформити заяви на соціальну допомогу чи інші пільги;
- реєстрація бізнесу та нерухомості. Підприємці громади мають можливість реєструвати свою діяльність або здійснювати зміни у реєстраційних даних без додаткових витрат часу;
- оформлення субсидій. Через ЦНАП мешканці можуть подати документи для оформлення житлових субсидій, що значно спрощує доступ до цієї послуги.

ЦНАП працює за принципом "єдиного вікна", що означає, що всі необхідні послуги можна отримати в одному місці. Це усуває необхідність звертатися до кількох різних установ, скорочуючи час і зменшуючи адміністративне навантаження на громадян.

Окрім того, центр оснащений сучасною технікою та програмним забезпеченням, що дозволяє автоматизувати багато процесів і зменшити можливість помилок. Персонал ЦНАП регулярно проходить навчання, щоб

забезпечити високий рівень обслуговування та професійний підхід до вирішення питань.

Завдяки роботі ЦНАП Підгородненська міська громада забезпечує своїм мешканцям комфортний доступ до адміністративних послуг, підвищуючи рівень задоволення потреб громадян і підтримуючи ефективну взаємодію між громадою та місцевими органами влади.

Цей підхід забезпечує прозорість роботи органів місцевого самоврядування та сприяє залученню громадян до участі в розвитку громади, покращуючи взаєморозуміння між владою та мешканцями.

Окрім того за ініціативи Підгородненської міської ради реалізується Програма інформатизації, яка очікується буде реалізовано до 2025 року. Дана програма направлена на подальший розвиток електронного урядування та електронної демократії.

Таким чином, Підгородненська міська рада забезпечує належний рівень інформаційного забезпечення, використовуючи як традиційні, так і сучасні цифрові канали комунікації для взаємодії з громадою.

2.3. Виявлення основних проблем і недоліків інформаційного забезпечення Підгородненської міської ради в умовах воєнного стану

Реальний стан інформаційного забезпечення Підгородненської міської ради в умовах воєнного стану можна проілюструвати практичними прикладами, які демонструють як наявні досягнення, так і проблеми.

Система обліку переселенців. У міській раді створено базу даних для реєстрації внутрішньо переміщених осіб (ВПО), яка дозволяє відслідковувати їхні потреби у житлі, гуманітарній допомозі та соціальній підтримці. Однак через відсутність інтеграції з іншими системами, наприклад, обласними чи державними, ця база працює автономно. Це ускладнює координацію з іншими органами влади та затримує розподіл ресурсів.

Комунікація з громадянами через соціальні мережі. У період регулярних повітряних тривог міська рада використовує свою сторінку у Facebook для оперативного інформування населення про небезпеку або важливі події. Наприклад, громадян повідомляли про час і місце видачі гуманітарної допомоги. Проте обмежене охоплення аудиторії в соціальних мережах та відсутність стабільного Інтернет-зв'язку в окремих районах громади обмежують ефективність такого інструменту.

Недосконалий документообіг. Процеси внутрішнього документообігу, наприклад, реєстрація звернень громадян чи запитів від волонтерських організацій, все ще частково ведуться у паперовій формі. Це уповільнює обробку запитів, особливо у разі одночасного надходження великої кількості звернень.

Захист інформації та кіберзагрози. У 2023 році міська рада зазнала кількох спроб несанкціонованого доступу до своїх систем. Хоча базові заходи кібербезпеки (зміна паролів, антивірусний захист) змогли відбити атаки, відсутність сучасних систем моніторингу та реагування на кіберзагрози залишає інформаційні ресурси вразливими.

Гуманітарна координація. У перші місяці війни рада створила тимчасову інформаційну гарячу лінію для координації видачі гуманітарної допомоги. Однак через обмежену кількість операторів ця лінія швидко переважувалася, що призводило до затримок у наданні інформації.

Реєстр житлового фонду для ВПО. З ініціативи міської ради розроблено таблицю в Excel для обліку житлових приміщень, доступних для розміщення переселенців. Однак її ручне оновлення призводило до частих помилок, які ускладнювали розподіл місць.

Таким чином, хоча Підгородненська міська рада здійснює значні зусилля для забезпечення інформаційної підтримки в умовах воєнного стану, реальні приклади показують, що існує потреба у більшій цифровізації, покращенні кібербезпеки, інтеграції систем і розширенні доступу до інформації.

В умовах воєнного стану Підгородненська міська рада стикається з багатьма проблемами в інформаційному забезпеченні, які впливають на ефективність її роботи та взаємодію з громадянами.

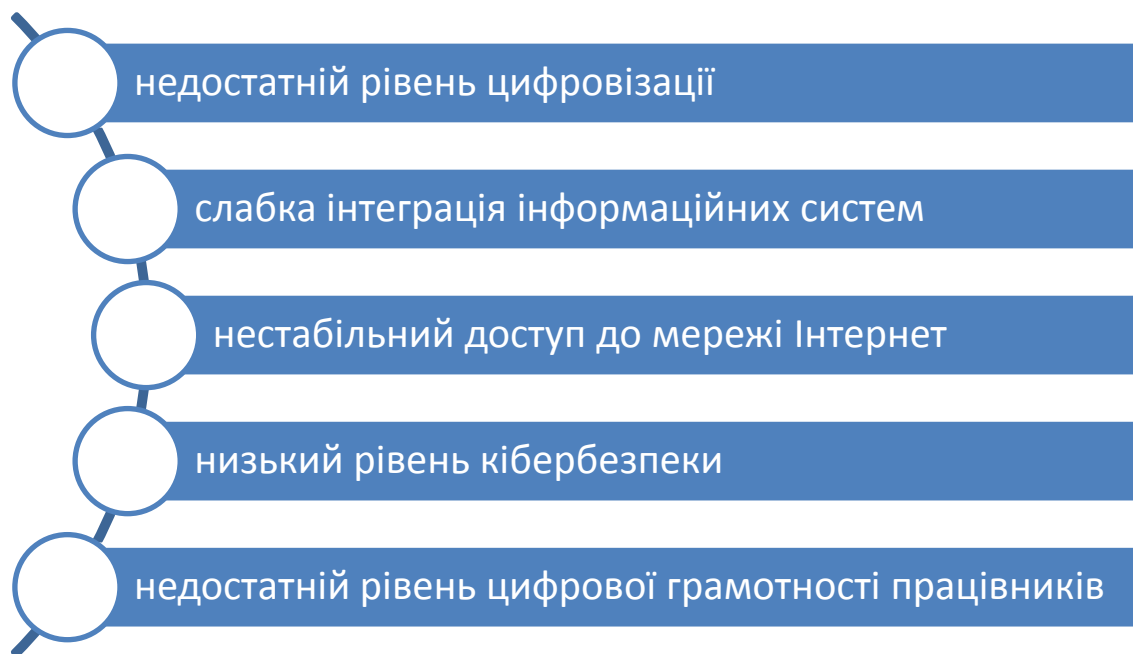


Рис. 2.3. Основні проблеми в інформаційному забезпеченні у Підгородненській міській раді

Однією з основних проблем є недостатній рівень цифровізації. Багато процесів досі виконуються вручну або з використанням застарілих технологій, що уповільнює обробку інформації та прийняття рішень. Відсутність єдиної централізованої бази даних призводить до складнощів у доступі до актуальної інформації, необхідної для управління.

Ще однією серйозною проблемою є слабка інтеграція інформаційних систем. Підрозділи міської ради часто працюють у відокремлених системах, які не синхронізуються між собою. Це створює труднощі у передачі даних і координації роботи між відділами. Наприклад, різні служби можуть використовувати окремі бази даних, що ускладнює спільну роботу над вирішенням питань громади.

Крім того, у деяких частинах громади спостерігаються перебої з доступом до Інтернету, що обмежує можливості використання сучасних технологій. Це впливає як на внутрішню роботу ради, так і на зв'язок із жителями громади, особливо в умовах, коли оперативне інформування населення є критично важливим.

Ще одним важливим недоліком є недостатня кібербезпека. Відсутність належного рівня захисту інформаційних систем створює ризики несанкціонованого доступу до даних або їх втрати, що особливо небезпечно в умовах зростання кібератак під час воєнного стану. Ці загрози можуть паралізувати роботу важливих сервісів та підірвати довіру громадян до органів місцевого самоврядування.

Також варто зазначити, що рівень цифрової грамотності працівників міської ради залишається низьким. Це ускладнює впровадження нових технологій та ефективне використання наявних інструментів. Багато співробітників не володіють необхідними навичками для роботи з сучасними системами, що додатково уповільнює процеси.

В цілому, основні проблеми інформаційного забезпечення в Підгородненській міській раді включають недостатню цифровізацію, слабку інтеграцію систем, нерівномірний доступ до Інтернету, загрози кібербезпеці та низький рівень цифрової грамотності. Вирішення цих проблем вимагає системного підходу, включаючи модернізацію технологій, навчання персоналу та впровадження комплексних заходів із захисту інформації.

Висновки до розділу 2

1. Інформаційне забезпечення в умовах воєнного стану потребує чіткого правового регулювання, яке враховує специфіку кризових умов. Впровадження нормативно-правових актів, таких як Закон України «Про правовий режим воєнного стану» та укази Президента, забезпечує координацію роботи органів влади, захист інформаційного простору та

реалізацію єдиної інформаційної політики. Водночас, додаткові заходи, спрямовані на протидію дезінформації та забезпечення кібербезпеки, є критично важливими для збереження національної безпеки.

2. Підгородненська міська рада активно впроваджує сучасні інформаційні технології, використовуючи офіційний веб-сайт та соціальні мережі для інформування мешканців та забезпечення прозорості своєї діяльності. Важливу роль відіграє ЦНАП, який надає широкий спектр адміністративних послуг. Однак громада потребує подальшого розвитку інформаційної інфраструктури, вдосконалення електронного документообігу та інтеграції цифрових сервісів для підвищення ефективності управління.

3. Основними проблемами інформаційного забезпечення є недостатня цифровізація, відсутність інтеграції між інформаційними системами, нерівномірний доступ до Інтернету, низький рівень кібербезпеки та недостатня цифрова грамотність працівників. Ці фактори уповільнюють процеси управління, ускладнюють комунікацію з громадянами та підвищують ризики для збереження інформації. Для їх вирішення необхідно модернізувати технології, впровадити нові методи кіберзахисту, підвищити рівень цифрової грамотності персоналу та забезпечити безперервний доступ до Інтернету в усіх частинах громади.

РОЗДІЛ 3.

НАПРЯМИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Іноземний досвід інформаційного забезпечення органів державної влади

Інформаційне суспільство розвивається по-різному залежно від національних особливостей, таких як менталітет, політична система, економіка та соціальні умови. У США ключову роль в інформаційному співтоваристві відіграють національна інформаційна інфраструктура та цифрова економіка, які тісно взаємопов'язані. Європейські країни підходять до інформаційного суспільства через такі фактори, як інтеграція економіки, розвиток національної інформаційної інфраструктури, затребуваність інформаційних ресурсів і забезпечення вільної конкуренції.

США накопичили значний досвід у сфері інформаційного забезпечення управлінських процесів, який може бути корисним для України. Історично інтернет-ресурси в США спершу використовувалися оборонними структурами, наприклад, мережею ARPAnet, створеною для Пентагону. Далі «Кремнієва долина» стала символом американського технологічного прориву завдяки реалізації «Вашингтонського консенсусу». Ця модель розвитку передбачала зменшення державного втручання в економіку, застосування податкових пільг і стимулювання реальної конкуренції. Такі зміни дозволили приватному бізнесу долучитися до оборонних програм, що призвело до активного впровадження інформаційних технологій у підприємництво. Це стало основою для інформаційної революції [50].

Попри те, що спочатку не вистачало нормативно-правової бази для регулювання використання інформаційних ресурсів і технологій, уряд США оперативно розробив відповідне законодавство. Це забезпечило участь

органів влади в процесі інформатизації та запобігло інформаційній кризі. Завдяки цим зусиллям США стали лідером у використанні Інтернет-технологій, маючи високі показники швидкості передачі даних, кількості комп'ютерів і чисельності користувачів.

У результаті був створений «Електронний уряд», що значно підвищив ефективність взаємодії між державою і населенням. Він надав низку інструментів для адміністративних і державних реформ, таких як система авторизації доступу, пошукові сервіси для інформаційних ресурсів, платформи для федеральних закупівель і заповнення форм. Це стало прикладом ефективного використання цифрових технологій для оптимізації державного управління [12].

У європейських країнах був реалізований проєкт під назвою «Технологія формування та розвитку інформаційного суспільства», що став частиною П'ятої рамкової програми, спрямованої на дослідження у сфері інформаційних технологій. Однак перший рік реалізації цього проєкту виявився неуспішним, через що результати були визнані незадовільними. У відповідь на це Європейська комісія розробила новий стратегічний документ під назвою «Електронна Європа». Ця ініціатива мала на меті створення об'єднаного інформаційного суспільства на міждержавному рівні, що сприяло б інтеграції країн Європи в умовах інформаційної революції. До ключових завдань «Електронної Європи» були віднесено такі:

- формування інфраструктурного інформаційно-комунікаційного простору;
- вільний вхід у цей простір усіх зацікавлених користувачів;
- нормативно-правове забезпечення інформаційних проєктів: «Мультимедійна комунікація», «Електронна комерція», «Захист угоди»;
- ефективне функціонування електронного уряду у різних його формах;
- підвищення професіоналізму, освіченості та кваліфікованості всіх громадян;

- формування та підтримання у робочому стані глобальна мережа Європейського Союзу [8].

Ключові цілі програмних матеріалів у західних країнах орієнтовані на досягнення лідерства в економічній, соціальній та духовній сферах. В основі таких програм стоїть особистість із її потребами, інтересами та запитами. Мета цих програм — забезпечення соціально-економічного розвитку для підвищення рівня добробуту населення.

У європейських країнах розвиток заснований на формуванні довіри громадян до інформаційних технологій у державному управлінні, а також на підтримці малого та середнього бізнесу. Особливу увагу приділяють створенню електронних урядів та інтеграції їх із системами електронної комерції в єдину он-лайн-технологію, що стає фундаментом цифрової економіки.

У порівнянні із західними країнами підходи до побудови інформаційного суспільства в Україні мають свої особливості, які базуються на політичному, економічному та соціальному контексті. Західні держави орієнтуються на людину як центральний елемент розвитку, акцентуючи увагу на її потребах, запитах і соціально-економічному добробуті. Ці країни активно впроваджують електронні уряди, розвивають електронну комерцію та інтегрують їх у єдину цифрову інфраструктуру. Це дозволяє забезпечити високу ефективність державного управління, покращити доступ громадян до послуг та стимулювати розвиток малого й середнього бізнесу.

В Україні, особливо в останнє десятиліття, також спостерігається значний прогрес у цифровізації. Уряд впроваджує сучасні технології для покращення взаємодії між державними органами та громадянами. Наприклад, платформа "Дія" стала важливим кроком у створенні електронного уряду, дозволяючи громадянам отримувати державні послуги он-лайн. Це наближає Україну до західної моделі інформаційного суспільства, орієнтованої на громадянські потреби.

Проте на відміну від розвинених західних країн, в Україні процеси цифровізації ще стикаються з низкою викликів, таких як нерівномірний доступ до Інтернету, недостатня цифрова грамотність населення та обмежені ресурси для реалізації масштабних цифрових ініціатив. Крім того, в умовах воєнного стану акцент робиться на забезпеченні кібербезпеки та захисті критичної інфраструктури, що є пріоритетом на рівні державного управління.

Однією з ключових відмінностей є масштаби та інтеграція. У західних країнах цифрова інфраструктура вже давно стала основою для побудови інформаційного суспільства, тоді як Україна лише формує цю базу. Водночас в Україні цифровізація часто реалізується швидкими темпами, що дозволяє уникнути багатьох перехідних етапів, які свого часу проходили західні країни.

Для України найбільш корисним досвідом може стати поєднання практик різних країн, які успішно реалізували цифровізацію та модернізацію державного управління. Зокрема, досвід Естонії є одним із найкращих прикладів для України. Естонія створила ефективну систему електронного уряду, яка дозволяє громадянам отримувати більшість державних послуг онлайн, використовувати електронну ідентифікацію, реєструвати бізнес чи навіть голосувати на виборах через Інтернет. Це значно спростило взаємодію громадян із державою та підвищило ефективність управління.

Україні варто взяти на озброєння естонську модель інтегрованих баз даних та платформ для обміну інформацією між державними органами. Це дозволило б забезпечити прозорість, зменшити бюрократію та прискорити надання послуг.

Також цікавим є досвід Фінляндії у створенні цифрових освітніх платформ, які адаптуються до потреб різних груп населення. Україна, яка приділяє значну увагу реформуванню освіти, може застосувати подібний підхід, щоб забезпечити доступ до якісних освітніх ресурсів у всіх регіонах, включно з тими, які постраждали від війни.

Зі свого боку, досвід США у розвитку інноваційної екосистеми та підтримці підприємництва через податкові стимули й венчурне фінансування також може бути корисним. Це допомогло б Україні стимулювати розвиток ІТ-галузі та стартапів, які є ключовими гравцями у сучасній цифровій економіці.

Загалом, Україні варто зосередитися на інтеграції електронного уряду, покращенні доступу до Інтернету, розвитку цифрових навичок населення та залученні міжнародного досвіду для захисту критичної інформаційної інфраструктури, що є надзвичайно важливим у поточних умовах.

3.2. Забезпечення кібербезпеки та захисту інформаційних потоків органів державної влади

Кібербезпека – це захист життєво важливих інтересів людини і громадянина, суспільства і держави під час використання кіберпростору. Це забезпечує сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, а також запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України в кіберпросторі.

Кібербезпека відіграє критично важливу роль у сучасному світі, оскільки вона забезпечує захист ключових інтересів людини, суспільства та держави в умовах стрімкої цифровізації. У сучасному інформаційному середовищі майже всі аспекти життя, від персональних даних до державних ресурсів, залежать від безпеки в кіберпросторі.

Забезпечення кібербезпеки є важливим для сталого функціонування інформаційного суспільства, адже вона дозволяє захищати електронні ресурси від несанкціонованого доступу, атак чи порушення їхньої роботи. Це особливо актуально для захисту державної інфраструктури, банківських систем, об'єктів критичної інфраструктури, а також приватних компаній і персональних даних громадян [6].

Крім того, кібербезпека є фундаментальною складовою національної безпеки. В умовах зростаючих кіберзагроз, таких як хакерські атаки, поширення шкідливого програмного забезпечення, фішинг чи DDoS-атаки, держава зобов'язана забезпечити захист своїх громадян, інформаційних ресурсів та ключових систем від потенційних ризиків.

Важливість кібербезпеки також пов'язана з довірою до цифрових технологій і електронних послуг. Надійний захист інформації сприяє підвищенню довіри громадян до державних і приватних сервісів, створює передумови для розвитку цифрової економіки, електронного урядування та сучасних комунікацій.

Основні поняття та принципи національної кібербезпеки України визначено в Законі України «Про основи кібербезпеки України» від 5 жовтня 2017 р. Відповідно до цього Закону «кібербезпека – це стан захищеності критичної інформаційної інфраструктури, інформаційних ресурсів, інформаційних систем і мереж від кіберзагроз. Забезпечення кібербезпеки в Україні базується на принципах:

- верховенство права, законність, повага до прав людини і основних свобод та їх захист у встановленому законом порядку;
- національний суверенітет, територіальну цілісність і недоторканність кордонів України;
- єдність державної політики у сфері кібербезпеки;
- партнерство органів державної влади, органів місцевого самоврядування, суб'єктів господарювання та громадянського суспільства у забезпеченні кібербезпеки;
- взаємодопомога та співпраця з іншими державами та міжнародними організаціями у сфері кібербезпеки;
- пропорційність заходів кібербезпеки реальному стану загроз у кіберпросторі;
- прозорість та взаємоконтроль державних органів, що забезпечують кібербезпеку» [35].

Стратегія кібербезпеки України визначає пріоритети національних інтересів у сфері кібербезпеки, існуючі та потенційно можливі загрози, цілі та завдання держави щодо забезпечення кібербезпеки.

Забезпечення національної кібербезпеки потребує комплексного підходу, що включає різноманітні засоби та методи захисту. Деякі з них включають:

- реалізація Стратегії кібербезпеки України, яка визначає цілі та пріоритети державної політики у цій сфері, а також механізми її реалізації;
- створення та функціонування національної системи кібербезпеки, яка об'єднує різні суб'єкти, що забезпечують кіберзахист державних інформаційних ресурсів, критичної інфраструктури, банківської системи, сектору оборони та безпеки тощо;
- застосування стандартів і правил у сфері кібербезпеки, які встановлюють вимоги до захисту інформації, мереж, систем, пристроїв, програмного забезпечення тощо;
- використання сучасних технологій та інструментів кібербезпеки, що дозволяють виявляти, запобігати, локалізувати та усувати кібератаки, а також відновлювати нормальну роботу комп'ютерних систем та мереж;
- проведення просвітницько-інформаційних заходів для підвищення рівня обізнаності та компетентності громадян, державних службовців, працівників суб'єктів національної системи кібербезпеки тощо щодо загроз та заходів захисту у цій сфері [36].

Відповідно, Україні для розвитку власної системи кібербезпеки необхідно враховувати досвід і перспективи розвитку систем кібербезпеки НАТО та окремих країн НАТО. Також вихідними даними для побудови ефективної системи кібербезпеки, як на державному рівні, так і для Міністерства оборони України та Збройних Сил України, мають бути: Загрози кібербезпеці України, насамперед з боку Російської Федерації, а також міжнародних хакерських організацій; Власний досвід, розробки та

технології забезпечення кібербезпеки; Результати об'єктивної оцінки стану українського сегменту кіберпростору та можливостей суб'єктів кібербезпеки.

Забезпечення кібербезпеки та захисту інформаційних потоків органів державної влади є критично важливим завданням, особливо в умовах підвищених загроз. Для цього необхідно впроваджувати комплексні заходи, які включають як технічні, так і організаційні рішення [7].

Органам влади слід забезпечити використання сучасних технологій шифрування даних для захисту конфіденційної інформації під час передачі через мережі. Важливо регулярно оновлювати програмне забезпечення та системи безпеки, щоб уникнути використання вразливостей, які можуть бути наявними у застарілих версіях. Також доцільно розгорнути системи виявлення та реагування на кіберзагрози, що дозволяють оперативно реагувати на спроби несанкціонованого доступу або атаки.

Необхідно посилити контроль за доступом до критичних інформаційних ресурсів. Це включає впровадження багаторівневої аутентифікації для користувачів, управління доступом на основі ролей і регулярний моніторинг активності в мережах. Проведення аудитів безпеки також є важливим інструментом для виявлення та усунення потенційних ризиків.

Особливу увагу слід приділяти навчанню працівників органів державної влади. Їх потрібно інформувати про основні правила кібергігієни, розпізнавання фішингових атак і правильне використання захищених каналів зв'язку. Важливо створити чіткі протоколи реагування на кіберінциденти, щоб забезпечити злагодженість дій у разі кризової ситуації.

Інвестиції в резервування даних є ще одним ключовим елементом. Регулярне створення резервних копій та їхнє зберігання в захищених сховищах забезпечить збереження інформації навіть у разі успішної атаки чи технічної несправності.

Окрім того, слід розширювати співпрацю з міжнародними партнерами та організаціями, які займаються кібербезпекою, для обміну досвідом і

ресурсами. Це дозволить запозичити кращі практики та швидко адаптуватися до нових загроз. Важливо також забезпечити належну координацію між різними органами державної влади, щоб уникнути прогалин у кіберзахисті та посилити єдину національну кібербезпекову інфраструктуру.

Для цього пропонуємо розробити Програму забезпечення та розвитку кібербезпеки Підгороднінської міської ради та жителів громади

Мета програми - підвищення рівня кібербезпеки органів державної влади шляхом впровадження сучасних технологій, стандартів та процедур для захисту інформаційних ресурсів, забезпечення стійкості до кіберзагроз та гарантування безперервності функціонування.

Основними завданнями є наступні:

- розробка та впровадження єдиної стратегії кібербезпеки Підгородненської міської ради та громади;
- забезпечення захисту інформаційних систем і даних Підгородненської міської ради;
- розвиток інфраструктури резервного копіювання та відновлення даних Підгородненської міської ради;
- підвищення рівня обізнаності працівників Підгородненської міської ради у сфері кібербезпеки;
- впровадження новітніх технологій для моніторингу, виявлення та реагування на кіберінциденти;
- співпраця з міжнародними організаціями та партнерами для посилення національної кібербезпеки;

Вважаємо, що реалізація зазначеної програми дозволить отримати наступні результати:

- стабільне функціонування інформаційних систем органів державної влади навіть у разі кібератак;
- зниження ризику витоку або втрати даних;
- підвищення довіри громадян до державних електронних сервісів;
- створення професійної спільноти фахівців із кібербезпеки.

Таблиця 3.1

Програма розвитку кібербезпеки Підгородненської міської ради

Етапи реалізації	Заходи
Етап 1: Аналіз та оцінка (1-6 місяців)	<ul style="list-style-type: none"> - Проведення повного аудиту інформаційної безпеки органів державної влади. - Оцінка вразливостей інформаційних систем, програмного забезпечення та мереж. - Ідентифікація основних загроз і ризиків, які можуть вплинути на безпеку даних. - Розробка рекомендацій для усунення недоліків у захисті інформаційних ресурсів. - Створення карти кіберзагроз для державних установ.
Етап 2: Розробка та стандартизація (6-12 місяців)	<ul style="list-style-type: none"> - Розробка єдиного стандарту кібербезпеки для органів державної влади. - Встановлення регламентів зберігання, обробки та передачі конфіденційної інформації. - Впровадження політики управління доступом, що базується на ролях та потребах працівників. - Встановлення систем багаторівневої аутентифікації (включаючи використання токенів або біометрії). - Затвердження правил реагування на кіберінциденти та створення відповідних процедур
Етап 3: Інфраструктурні зміни (1-2 роки)	<ul style="list-style-type: none"> - Модернізація обладнання та програмного забезпечення для забезпечення високого рівня безпеки. - Розгортання сучасних систем моніторингу мережі для виявлення кіберзагроз у реальному часі. - Створення інфраструктури для регулярного резервного копіювання даних та їхнього відновлення. - Впровадження шифрування даних під час зберігання та передачі. - Забезпечення безперебійного доступу до резервних серверів у разі кібератаки чи технічної несправності.
Етап 4: Навчання та підвищення кваліфікації (1-3 роки)	<ul style="list-style-type: none"> - Проведення регулярних тренінгів для працівників державних установ з кібергігієни та розпізнавання загроз (наприклад, фішингових атак). - Організація навчальних симуляцій кіберінцидентів для перевірки готовності до реагування. - Впровадження програм сертифікації для спеціалістів із кібербезпеки, які працюють у державних установах. - Проведення інформаційних кампаній щодо новітніх загроз у сфері кібербезпеки.

Ці етапи забезпечать системний і поетапний підхід до впровадження програми кібербезпеки, що дозволить досягти високої ефективності в захисті інформаційних потоків органів державної влади.

3.3. Рекомендації щодо посилення комунікації між державними органами і громадянами в умовах воєнного стану

Стратегічне питання для української держави є «створення ефективної системи державного управління, що є передумовою успішної реалізації функцій державного управління, надання якісних адміністративних послуг, належної співпраці з інститутами громадянського суспільства та входження України до світового співтовариства як правової, соціальної та демократичної держави» [42].

«Україна, з усіма суперечностями та конфліктами, які виникають на етапі розвитку глобального інформаційного суспільства, потребує вироблення цілісної стратегії у сфері державної політики з використанням модернізованих інформаційно-комунікаційних механізмів на основі нової парадигми суспільного розвитку та його сучасної ціннісно-орієнтаційні принципи. Водночас реалізація комунікаційного механізму в системі державного управління та в державі загалом, що особливо важливо в плюралістичному суспільстві, стає вирішальним. Тому комунікація є основним «енергетичним двигуном», який забезпечує безперервну роботу всієї системи та виконує стратегічні завдання щодо забезпечення реалізації певної мети» [24].

Проте низка проблем, зумовлених політичними, соціокультурними, комунікативними, правовими, організаційними, освітніми чинниками, гальмує формування позитивного іміджу органів державної влади в Україні, особливо в умовах воєнного стану.

«Сучасний імідж органів державної влади в Україні характеризується недостатньою довірою суспільства та потребує інтенсивного пошуку нових форм взаємодії влади та суспільства, які сприяли б посиленню спроможності органів державної влади налагоджувати діалог та якісні стосунки з різними соціальними групами». [21].

Діалог відіграє важливу роль у вирішенні конфліктів, гармонізації суспільних відносин і досягненні національного консенсусу. Основні завдання комунікаційних підрозділів публічного сектору влади, належне виконання яких сприятиме формуванню позитивного іміджу органів державної влади в умовах воєнного стану, систематизовано на рис. 3.1.

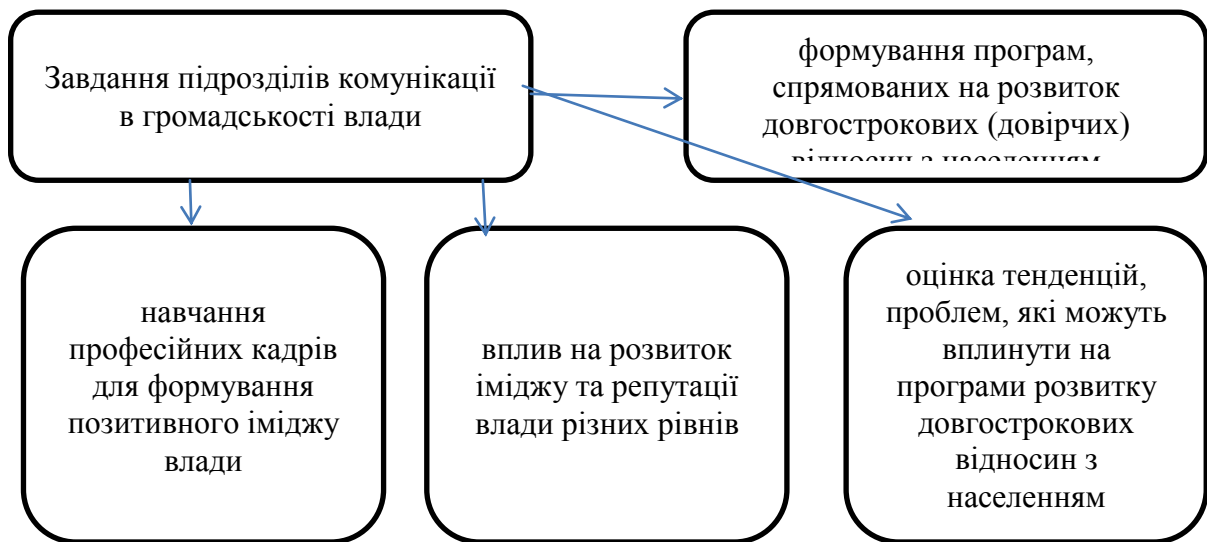


Рис. 3.1. Завдання комунікаційних підрозділів в органах державної влади

Розвиток якісних інформаційно-комунікаційних механізмів в Україні ускладнюється ще й тим, що питання взаємодії державних установ, органів місцевого самоврядування, ЗМІ та громадськості «розпорошені» у багатьох нормативно-правових актах, частина з яких є рішеннями Кабінету Міністрів. З огляду на це важливі інструменти комунікації (громадські консультації, громадська експертиза тощо) стосуються лише виконавчої влади.

Питання налагодження взаємодії громадськості та влади, особливо в діяльності центральних органів виконавчої влади, може бути частково вирішено шляхом розробки таких інформаційно-комунікаційних механізмів, які б формували позитивний імідж органів державної влади та базувалися на принципі взаємної взаємодії. відповідальність. Тобто влада зобов'язується бути відкритою, оприлюднювати свої політичні рішення, забезпечувати їх

прозорість і доступність для громадськості, проводити консультації при виробленні та реалізації державної політики, налагоджувати та розвивати публічний діалог.

Інститути громадянського суспільства відіграють важливу та активну роль у розробці державної політики і можуть здійснювати контроль за діяльністю органів державної влади. Формування та подальший розвиток моделі вдосконалення інформаційно-комунікаційних механізмів для формування позитивного іміджу органів державної влади в Україні має здійснюватися за чотирма ключовими напрямками:

- розширення взаємодії з громадськістю;
- зміцнення співпраці між державною владою та засобами масової інформації;
- удосконалення процесу надання державних послуг;
- оптимізація кадрових процесів;
- розширення взаємодії з громадськістю [4] .

На сьогодні значною проблемою є зниження рівня довіри громадян до діяльності органів державної влади, що обумовлено недостатнім використанням інформаційно-комунікаційних технологій та неефективністю існуючих механізмів їх роботи. [24].

Застосування інформаційно-комунікаційних технологій в роботі органів державної влади створює умови для посилення громадської участі в політичному житті країни, активізації громадської діяльності та розвитку електронної демократії, зокрема через:

- ефективне застосування сучасних інформаційно-комунікаційних технологій для забезпечення участі громадян і незалежних організацій у формуванні та реалізації державної політики, а також для підтримки громадськістю пілотних Інтернет-проектів;
- розробку методологічних і практичних основ комунікативної культури органів влади у процесі переходу до нового стилю державного управління;

– використання засобів масової інформації для створення дискусійної платформи, на якій громадяни можуть відстоювати та захищати суспільні інтереси.

Створення єдиної системи інформаційно-комунікаційної діяльності державних установ України та забезпечення комплексної координації її складових в органах державної влади вимагає прийняття низки державних рішень, які сприятимуть формуванню позитивного іміджу органів влади, особливо в умовах воєнного стану. Інші пропозиції щодо подальшого вдосконалення інформаційно-комунікаційних механізмів формування позитивного іміджу органів державної влади в Україні наведено в таблиці 3.2.

1. Посилення взаємодії між державною владою та засобами масової інформації є ключовим чинником у формуванні іміджу органів влади, оскільки інформаційно-комунікаційна діяльність відіграє важливу роль у створенні громадської думки. З урахуванням зростання світового інформаційного ринку, ЗМІ стають основним осередком, де відбуваються численні суспільно-політичні події, накопичуються різноманітні повідомлення, а також формується механізм впливу на суспільну свідомість. У цьому контексті органи державної влади активно використовують засоби масової інформації та пов'язані з ними комп'ютерні та інформаційні технології для створення позитивного образу серед громадськості.

Формування іміджу різних державних установ через засоби масової інформації створює стабільні читацькі та аудиторські вподобання, що, в свою чергу, впливає на розвиток суспільних цінностей. Недостатня або повна відсутність інформації про діяльність органів державної влади спричиняє незрозуміння політики з боку громадськості та виникнення негативних стереотипів щодо влади. Інформаційно-комунікаційна діяльність і засоби масової інформації є основними інструментами комунікації, які дозволяють втілювати політичні ідеї та покращувати імідж державних інституцій. [21].

Таблиця 3.2.

Пропозиції щодо подальшого вдосконалення інформаційно-комунікаційних механізмів формування позитивного іміджу органів державної влади

Проведення комплексного аналізу громадської думки	Запровадження сучасних алгоритмів постійного аналізу громадської думки щодо дій усіх державних органів з використанням таких форм інформаційно-комунікаційних технологій, як залучення професійних соціологічних служб; розробка анонімних анкет; проведення онлайн-опитувань, моніторингу листів та скарг громадян. За результатами опитування громадської думки – прийняття відповідного державного управління рішення, яке необхідно оприлюднити в ЗМІ
Удосконалення системи видавничої справи інформація про громадські запити	Удосконалення системи «гарячих ліній», «поштових скриньок», громадських приймалень, куди громадяни можуть надати інформацію про всі негативні факти в діяльності органів державної влади та внести пропозиції щодо усунення недоліків. Запровадити обов'язкову публікацію результатів реагування на звернення громадян шляхом розміщення відповідних матеріалів у засобах масової інформації, мережі Інтернет, на інформаційних стендах, у громадських місцях
Незалежне експертне регулювання діяльності органів державної влади	Створення умов для ефективної діяльності Громадських рад при органах державної влади, залучення до їх діяльності впливових та компетентних фахівців у відповідних галузях знань, з метою усунення проблем та недоліків у діяльності органів державної влади.
Широке та доступніше інформування населення	Розміщення рекламно-інформаційних матеріалів на веб-сайтах органів державної влади
Проведення дискусій щодо прийняття суспільно значущих рішень між суспільством і владою	Регулярно проводяться консультації освічених спеціалістів органів державної влади, а також представників громадськості, журналістів «круглих столів», участь у програмах на радіо та телебаченні для розуміння подальших шляхів розвитку спільних відносин з населенням.
Створення умов для організації та проведення регулярних зборів громадян та органів влади	Створення обов'язкової та регулярної системи комунікації державних установ з громадськістю, проведення зустрічей з цільовою аудиторією, представниками громадських організацій, представниками популярних ЗМІ, організація прямих ефірів з можливістю зворотного зв'язку тощо.

Таким чином, засоби масової інформації є частиною розвитку інформаційно-комунікаційного механізму формування позитивного іміджу державних інституцій. Злагожені та злагожені дії представників ЗМІ,

змістовні та сучасні програми щодо своєчасного висвітлення актуальних суспільно-політичних та державних подій у суспільстві створюють позитивний імідж громадської установи.

Цей процес можна визначити як реалізацію тактичних і стратегічних кроків, які включають:

- планування, розробка, організація, обґрунтування та реалізація інформаційно-комунікаційної стратегії;
- пошук та визначення ключових і пріоритетних аспектів подальшого розвитку інформаційно-комунікаційної стратегії;
- підвищення «іміджу» публічної влади за рахунок використання найефективніших інструментів політичної комунікації.

Крім того, необхідно визначити рівень суспільної недовіри та апатії до роботи публічної адміністрації, сформований у суспільному розумінні через недостатню розвиненість ефективних інформаційно-комунікаційних механізмів [21]. Таким чином, для розробки інформаційно-комунікаційних механізмів формування позитивного іміджу у сфері взаємодії влади та в ЗМІ, необхідно сформулювати конкретні пропозиції (табл. 3.3).

Таблиця 3.3

Пропозиції щодо зберігання позитивного іміджу у сфері взаємодії влади та ЗМІ в умовах воєнного стану

Пропозиція	Зміст
Ефективне впровадження інформації та комунікаційна діяльність	На базі окремого підрозділу органу влади сформувати структуру, яка забезпечуватиме реалізацію інформаційної політики, аналіз та узагальнення питань, що негативно впливають на повноваження цього органу, з метою планування та координації організаційних і практичних заходів щодо створення позитивний імідж закладу
Постійний контроль за наданням відповідей на звернення громадян	Здійснювати постійний моніторинг звернень громадян щодо змісту, форми та напрямків донесення інформації до населення через засоби масової інформації. За результатами такого моніторингу спланувати підготовку відповідних матеріалів ЗМІ
Удосконалення системи засобів масової інформації	Удосконалити роботу системи відомчих ЗМІ телерадіопрограм, що зробить їх корисними та привабливими для суспільства.
Широке інформування населення	Інформувати громадськість про важливість PR-діяльності. Така обізнаність має підвищити імідж державних органів і, зокрема, поступово підвищити рівень довіри до органів державної влади та влади загалом.

Сьогодні громадяни вимагають від державних інституцій систематичності у їхній роботі для забезпечення легітимності та прозорості політики, особливо щодо проведення численних реформ, що частково або повністю залежать від взаємодії органів влади та засобів масової інформації. Важливу роль у цьому процесі відіграє підтримка громадянами діяльності державних органів на центральному та місцевому рівнях, що забезпечується, зокрема, ефективною співпрацею між місцевою владою та ЗМІ. Це сприяє розвитку та трансформації демократичної системи України та успішному впровадженню багатьох реформ. [15].

2. Удосконалення механізму надання державних послуг. Одним із перспективних напрямків розвитку механізмів управління послугами є мобільний доступ до їх отримання. Наразі створено умови для ефективного надання адміністративних послуг, є значні можливості для телефонної реверсивної технології «мобільного уряду». «Мобільний уряд» можна назвати ще одним кроком у створенні електронного уряду, який допоміг наблизити людей до влади. Це дозволило надавати послуги фізичним та юридичним особам, які користуються мобільним зв'язком.

Ключовим аргументом на користь розвитку електронного урядування є те, що доступ до Інтернету є не завжди доступним для всіх громадян, тоді як мобільні телефони використовуються більшістю людей. Це дозволяє встановити контакт з максимальною кількістю користувачів адміністративних послуг. «Мобільні уряди» можуть бути широко застосовані в різних сферах суспільного життя, надаючи громадянам можливість оплачувати різноманітні послуги (включаючи державні), брати участь у опитуваннях для покращення якості обслуговування, голосувати на виборах і контролювати їх процес, отримувати довідкову інформацію, сплачувати податки тощо. Загалом «мобільний уряд» може стати ефективним інструментом для встановлення двосторонніх відносин між владою та громадянами.

Для покращення комунікації з громадою та підвищення ефективності управлінських послуг можна запровадити СМС-сервіс, схожий на послуги мобільних операторів. Таке рішення забезпечить двосторонній потік інформації: з одного боку, органи державної влади надаватимуть корисну інформацію громадянам, зокрема в контексті адміністративних послуг; з іншого боку, громадяни зможуть звертатися до центрів надання адміністративних послуг для дистанційного отримання інформації або послуг, які не потребують особистого контакту з урядовцями. У разі необхідності особистого відвідування державних установ громадяни зможуть записатися в електронну чергу.

Сьогодні багато державних установ, у тому числі центри надання адміністративних послуг, встановили спеціальні термінали, за допомогою яких відвідувачі можуть, отримавши персональний номер, встановити порядок отримання послуги в електронному вигляді. На жаль, це значно зменшило черги в офісних будівлях і громадянам доводиться довго чекати. Проблему такого тривалого очікування можна вирішити, зареєструвавшись через sms-сервіс або мобільний додаток. Це дозволяє громадянину отримати однаковий номер у черзі та прийти у чітко визначений час, не витрачаючи зайвий час на використання спеціального терміналу.

По-перше, це підвищить задоволеність громадян якістю послуг, а по-друге, зменшить напругу в ЦНАП та дозволить адміністраторам працювати спокійно. У сучасному світі інформаційно-комунікаційні технології стали цінною інфраструктурною технологією для загального, а не лише індивідуального використання.

В даний час використання технологій електронного навчання стає пріоритетним напрямком навчання. «Електронне навчання вносить ряд інновацій у застосування сучасних інформаційно-комунікаційних технологій на основі мультимедіа. Важливо пам'ятати, що в умовах постійного оновлення інформаційно-комунікаційних технологій кожному громадянину важко розпізнати та опанувати великий потік інформації без спеціальних

навичок збору, пошуку, узагальнення, передачі та зберігання інформації. Саме тому в процесі становлення сучасного інформаційного суспільства особливу увагу слід приділяти практичному застосуванню інформаційно-комунікаційних технологій та компетентності державних службовців їх використовувати, адже лише фахівець, залучений до суспільних змін, може підвищити ефективність їх державно-управлінські аспекти» [44].

Найважливішим завданням державного менеджменту є оволодіння сучасними підходами до збирання, обробки та ефективного використання інформації, методів і засобів її оновлення. Від вирішення цього питання залежатиме своєчасність і невідкладність прийняття та реалізації державно-управлінських рішень щодо підтримки соціально-економічного зростання держави та підвищення соціального добробуту населення та країни в цілому.

У системі державного управління використовуються системи електронного документообігу, а представництво органів державної влади розвиває та вдосконалює надання послуг громадянам через Інтернет.

Однак реалізація цих кроків вимагає, по-перше, відповідних знань інформаційних експертів у сфері документообігу та інформаційних потоків. Ці фахівці повинні бути компетентними у впровадженні інформаційно-комунікаційних технологій та інформаційних систем для системної перебудови та ефективності суспільно значущої діяльності державного управління, що залежить не лише від рівня їх професіоналізму, а й від уміння використовувати сучасні автоматизовані системи управління. Курси підвищення кваліфікації керівників повинні проводитися регулярно з урахуванням розвитку комп'ютерної, офісної, організаційної та комунікаційної техніки.

«Аналіз можливостей використання сучасних інформаційно-комунікаційних технологій у реалізації інформаційно-аналітичного забезпечення державного управління дозволяє зробити висновок, що основні «резерви» підвищення його ефективності зосереджені в умінні використовувати всі методи аналітичної діяльності, стати більш надійним і

розумним» [18]. Водночас професійна підготовка державних службовців неможлива без практичного використання якісного та інноваційного інформаційного середовища. У такому середовищі керівник має значні перспективи отримання інформації, з одного боку, а з іншого – він повинен бути готовим «...швидко ідентифікувати та опрацьовувати великі обсяги інформації, оволодіваючи сучасними методами, техніками та технологіями» [23].



Рис. 3.2. Складові формування позитивного іміджу професійної діяльності керівників у контексті використання інформаційно-комунікаційних технологій

Напрями удосконалення кадрового механізму в контексті використання інформаційно-комунікаційних технологій

Пропозиції	Напрямки вдосконалення кадрового механізму
Сертифікаційне навчання	Організація навчальних курсів з управління інформаційно-комунікаційними технологіями має здійснюватися регулярно, враховуючи постійний розвиток комп'ютерної, офісної, організаційної та комунікаційної техніки, а також інновації у використанні технічних новинок у практиці державного управління.
Кадрове забезпечення	Підтримка формування позитивного іміджу влади, включаючи підготовку, перепідготовку та підвищення кваліфікації її представників у сфері інформаційно-комунікаційних технологій залежно від ступеня централізації державних процесів
Прозорість	Забезпечення чіткості та прозорості в діяльності органів державної влади шляхом здійснення управління на основі інтерактивного програмного забезпечення, з використанням сучасного апаратного та програмного забезпечення
Professionalism	Формування високого рівня професіоналізму та відповідальності в державному управлінні в результаті урізноманітнення форм інформації, забезпечення зворотного зв'язку та розширення можливостей для діалогу
Якість надання послуг	Надання державним службовцям якісних послуг, необхідних для виконання службових обов'язків та забезпечення законних інтересів, прав громадян, шляхом широкого використання в роботі державних службовців засобів наочності.
Критерії оцінки	Розробка прозорих та зрозумілих критеріїв оцінки ефективності діяльності державних службовців на основі використання спеціально розробленого програмного забезпечення, що економить час

Отже, державний службовець повинен володіти відповідною інформаційною культурою, яка є невід'ємною частиною всього інформаційного суспільства. Враховуючи це, стають актуальними питання поглиблення професійних знань і навичок органів влади, необхідних для виконання своїх обов'язків та надання якісних державних послуг. Це також включає забезпечення прав людини та громадянина шляхом індивідуалізації

освіти, підвищення якості подальшої освіти та надання переваги навчальним програмам європейського зразка. [23]. Систематизація особливостей використання компонентів інформаційно-комунікаційного механізму формування позитивного іміджу професійної діяльності керівника, представлена на рисунку 3.2.

Крім того, для ефективної реалізації складових формування позитивного іміджу професійної діяльності керівника, представлених на рис. 3.2, необхідне вдосконалення кадрового механізму в контексті використання інформаційно-комунікаційних технологій (табл. 3.3).

Отже, удосконалення інформаційно-комунікаційних механізмів формування позитивного іміджу має відбуватися за чотирма основними напрямками, зокрема: розширення системи зв'язків з громадськістю; посилення взаємодії державної влади та ЗМІ; удосконалення механізму надання державних послуг; оптимізація кадрового механізму, що сприятиме:

- більш широкому інформуванню населення про завдання та результати роботи органів державної влади;
- позитивне ставлення до рішень і дій державного управління;
- зростання у свідомості населення авторитету влади та довіри до неї;
- зменшення суспільного опору та нівелювання негативного стереотипу органів державної влади позитивної оцінки роботи органів державної влади через налагодження взаємовідносин між органами державної влади та громадськістю.

Для посилення комунікації між державними органами та громадянами в умовах воєнного стану важливо забезпечити оперативність, прозорість і доступність обміну інформацією. Це дозволить зміцнити довіру населення до влади, уникнути дезінформації та забезпечити координацію дій. Державні органи повинні активно використовувати сучасні технології, такі як соціальні мережі, месенджери, мобільні додатки та SMS-розсилки для оперативного інформування громадян. Особливо ефективними є платформи на кшталт

Telegram чи Facebook, де можна швидко поширювати важливі повідомлення, надавати інструкції та роз'яснення.

Важливо регулярно проводити публічні звернення представників влади через телебачення, радіо та інші доступні канали. Такі звернення мають бути чіткими, конкретними та спрямованими на зниження паніки серед громадян. Крім того, громадяни повинні мати можливість звертатися до гарячих ліній, які працюють цілодобово, надаючи консультації та допомогу. Для цього необхідно збільшити кількість операторів і забезпечити їх належною підготовкою.

Не менш важливим є створення централізованої інформаційної платформи, де можна отримати актуальну й офіційну інформацію в умовах воєнного стану. Це допоможе уникнути плутанини та поширення неправдивих новин. Залучення громадських організацій і волонтерів до комунікації також сприятиме поширенню важливих повідомлень серед різних верств населення, особливо тих, хто має обмежений доступ до Інтернету чи інших засобів зв'язку

Висновки до розділу 3

1. Іноземний досвід свідчить, що цифровізація державного управління, побудова електронних урядів і інтеграція інформаційних систем є ефективними інструментами для підвищення прозорості, доступності та ефективності роботи державних органів. США, Європейські країни та Естонія демонструють різні підходи до впровадження електронного уряду, які варто адаптувати до українських реалій. Україна вже зробила суттєві кроки в напрямку цифровізації, наприклад, через платформу "Дія", але залишається потреба у вирішенні таких проблем, як нерівномірний доступ до Інтернету, недостатня цифрова грамотність населення та обмежені ресурси.

2. Кібербезпека в умовах війни стає ключовим напрямом роботи державних органів. Для забезпечення захисту інформаційних потоків

необхідно впроваджувати сучасні технології шифрування, моніторингу загроз, резервного копіювання даних та багаторівневої аутентифікації. Крім того, важливо забезпечити навчання працівників органів влади основам кібергігієни та розробити чіткі протоколи реагування на кібератаки. Україна має орієнтуватися на міжнародний досвід, зокрема на стандарти НАТО, для посилення національної кібербезпеки.

3. Для ефективної комунікації між владою і громадянами в умовах воєнного стану важливо забезпечити прозорість, оперативність і доступність обміну інформацією. Використання сучасних інформаційно-комунікаційних технологій, таких як соціальні мережі, мобільні додатки, гарячі лінії та централізовані інформаційні платформи, допоможе уникнути дезінформації та підтримати довіру населення до влади. Регулярні публічні звернення представників влади, залучення громадських організацій та волонтерів також сприятимуть покращенню взаємодії з громадянами.

ВИСНОВКИ

1. Проаналізовано зміст поняття «інформаційне забезпечення» в державному управлінні. Встановлено, що інформаційне забезпечення є багатограним поняттям, яке об'єднує різні аспекти управління, технологій та права. Інформаційне забезпечення публічного управління можна розглядати як специфічний вид діяльності, що здійснюється інформаційними підрозділами органів влади з використанням сучасних інформаційно-комунікаційних технологій. Ця діяльність включає збір, обробку та аналіз даних для прийняття державних управлінських рішень і надання адміністративних послуг. Основними функціями, які виконує інформаційне забезпечення у публічному управлінні є: інформаційна, управлінська, діагностична, інструментальна, прогностична, під навальню-ментальна, безпекова.

2. Досліджено особливості інформаційного забезпечення в умовах кризових ситуацій та методологічні основи аналізу ефективності. Констатовано, що в умовах кризових ситуацій, таких як природні катастрофи, економічні потрясіння чи воєнний стан, інформаційне забезпечення органів державної влади стає надзвичайно важливим. Його завдання полягає в забезпеченні ефективного управління, швидкого прийняття рішень та координації дій на всіх рівнях. Основними ключовими особливостями інформаційного забезпечення є наступні: оперативність, достовірність, точність, безпечність інформації, доступність, системність, інерактивність, адаптивність, прозорість.

3. Проаналізовано стан нормативно-правового регулювання інформаційного забезпечення в умовах воєнного стану. Констатовано, що в умовах воєнного стану в Україні інформаційне забезпечення органів державної влади регулюється низкою нормативно-правових актів, які визначають порядок доступу до інформації, її захист та особливості функціонування інформаційних систем. Основою правового регулювання

залишаються такі ключові закони: Конституція України, Закон України «Про правовий режим воєнного стану», «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних» та інші акти, які визначають загальні принципи інформаційної діяльності. Однак в умовах воєнного стану додаються додаткові механізми для забезпечення безпеки інформаційних потоків.

4. Виявлено основні проблеми і недоліки інформаційного забезпечення органів державної влади в умовах воєнного стану. Дослідження проводилось на базі Підгородненської міської ради Дніпровського району Дніпропетровської області. Підгородненська міська рада активно використовує сучасні інформаційні технології для забезпечення прозорості своєї діяльності та ефективної комунікації з мешканцями громади. Основним інструментом є офіційний веб-сайт ради, де розміщуються новини, оголошення, рішення ради та виконавчого комітету, а також інша важлива інформація для громадян. Виявлені основні проблеми в інформаційному забезпеченні Підгородненської міської ради: недостатній рівень цифровізації, слабка інтеграція інформаційних систем, нестабільний доступ до мережі Інтернет, недостатній рівень кібербезпеки, недостатній рівень цифрової грамотності працівників. Вирішення цих проблем вимагає системного підходу, включаючи модернізацію технологій, навчання персоналу та впровадження комплексних заходів із захисту інформації.

5. Досліджено іноземний досвід інформаційного забезпечення органів державної влади. Констатовано, що у порівнянні із західними країнами, підходи до побудови інформаційного суспільства в Україні мають свої особливості, які базуються на політичному, економічному та соціальному контексті. Західні держави орієнтуються на людину як центральний елемент розвитку, акцентуючи увагу на її потребах, запитах і соціально-економічному добробуті. Ці країни активно впроваджують електронні уряди, розвивають електронну комерцію та інтегрують їх у єдину цифрову інфраструктуру. В

Україні процеси цифровізації ще стикаються з низкою викликів, таких як нерівномірний доступ до Інтернету, недостатня цифрова грамотність населення та обмежені ресурси для реалізації масштабних цифрових ініціатив. Крім того, в умовах воєнного стану акцент робиться на забезпеченні кібербезпеки та захисті критичної інфраструктури, що є пріоритетом на рівні державного управління. Отже, для України найбільш корисним досвідом може стати поєднання практик різних країн, які успішно реалізували цифровізацію та модернізацію державного управління

6. Надано пропозиції щодо удосконалення інформаційного забезпечення органів державної влади в умовах воєнного стану. Визначено, що забезпечення кібербезпеки є важливим для сталого функціонування інформаційного суспільства, адже вона дозволяє захищати електронні ресурси від несанкціонованого доступу, атак чи порушення їхньої роботи. Для забезпечення захисту інформаційних потоків необхідно впроваджувати сучасні технології шифрування, моніторингу загроз, резервного копіювання даних та багаторівневої аутентифікації. Крім того, важливо забезпечити навчання працівників органів влади основам кібергігієни та розробити чіткі протоколи реагування на кібератаки. Запропоновано для безпечної роботи Підгородненьської міської ради розробити Програму забезпечення та розвитку кібербезпеки, метою якої є підвищення рівня кібербезпеки органів державної влади шляхом впровадження сучасних технологій, стандартів та процедур для захисту інформаційних ресурсів, забезпечення стійкості до кіберзагроз та гарантування безперервності функціонування. Вважаємо, що реалізація зазначеної програми дозволить отримати наступні результати: стабільне функціонування інформаційних систем органів державної влади навіть у разі кібератак; зниження ризику витоку або втрати даних; підвищення довіри громадян до державних електронних сервісів; створення професійної спільноти фахівців із кібербезпеки.

7. Для ефективної комунікації між владою і громадянами в умовах воєнного стану важливо забезпечити прозорість, оперативність і доступність

обміну інформацією. Використання сучасних інформаційно-комунікаційних технологій, таких як соціальні мережі, мобільні додатки, гарячі лінії та централізовані інформаційні платформи, допоможе уникнути дезінформації та підтримати довіру населення до влади. Регулярні публічні звернення представників влади, залучення громадських організацій та волонтерів також сприятимуть покращенню взаємодії з громадянами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Амро Т. Взаємозв'язок систем забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану: методи та можливості. *Публічне урядування*. 2022. № (5 (33)), 83-88. [https://doi.org/10.32689/2617-2224-2022-5\(33\)-11](https://doi.org/10.32689/2617-2224-2022-5(33)-11)
2. Бондарчук Н.В., Полякова О.С., Стадник В.Г. Основи інформаційного забезпечення у формуванні молодіжної політики в умовах воєнного стану. Міжнародний науковий журнал «Інтернаука». 2024. № 11. <https://doi.org/10.25313/2617-572X-2024-11>
3. Глобенко С. Інформаційний простір держави та проблеми забезпечення його захисту в Україні. *Науковий вісник: Державне управління*. № 1 (13). 2023. С. 195–210.
4. Глущенко К. С. Імідж центральних органів виконавчої влади в системі комунікації з громадянським суспільством : дис. на здоб. канд. наук з держ. упр. 25.00.02 – механізми державного управління. Київ, 2018. С. 149.
5. Захарін, С. В., & Іщенко, І. С. (2023). Інформаційне забезпечення інноваційної діяльності суб'єктів господарювання в умовах існуючих викликів. *Проблеми сучасних трансформацій. Серія: економіка та управління*, (7). <https://doi.org/10.54929/2786-5738-2023-7-04-02>
6. Ісмайлов К.Ю. Поняття «кібербезпека» та «інформаційна безпека». Типологія безпеки. URL: <https://dspace.oduvs.edu.ua/items/92b9b4d1-5ee6-4d6d-bdf8-71645d3a485a>
7. Кисельов В. Впровадження сучасних інформаційно-комунікаційних технологій та вдосконалення інформаційного забезпечення в системах державного управління як нові стратегії адміністративних перетворень. *Наукові розвідки з державного та муніципального управління*. 2015. Вип. 1. С. 348–361

8. Клименко А.В., Гбур З.В. Інформаційне забезпечення органів публічної влади України. Інвестиції: практика та досвід. 2021. № 5. С.80-87. DOI: 10.32702/2306-6814.2021.5.80
9. Коваль Р.А. Інформаційне забезпечення діяльності органів державної влади в умовах глобалізації на регіональному рівні. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2016. №. 1. С. 103-111.
10. Конституція України від 28 червня 1996 року № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.
11. Копійка О. В. Інформаційна підтримка управлінських рішень в системі органів виконавчої влади. Науково–технічна інформація: наук.–практ. журнал. 2017. № 2. С. 6–12.
12. Кормич Б. А. Інформаційне право : підруч. [для студ. вищ. навч. закл.] / Б. А. Кормич. – Х. : БуруніК, 2011. – 333 с.
13. Кравець В.І., Слісаренко Т.В. (2017). Використання інформаційних технологій для підвищення ефективності управління підприємством. Науковий вісник Ужгородського національного університету. Ужгород: Гельветика. 13. 1. С. 136—140
14. Кравченко О.І. Інформаційна безпека як складова національної безпеки. Інвестиції: практика та досвід. 2023. № 18. С. 229-234.
15. Крюков О. І. До питання взаємодії публічної влади та засобів масової комунікації в сучасному політичному процесі. Вісник Національного Університету Цивільного Захисту: зб. наук. пр. Харків : Вид-во НУЦЗУ, 2018. Вип. 1 (8). (Серія «Державне управління»). С. 236–243
16. Лазарева К.В. (2020). Інформаційне забезпечення діяльності органів публічної влади. Правові засади організації та здійснення публічної влади: збірник тез III Міжнародної науково-практичної Інтернет-конференції, присвяченої світлій пам'яті доктора юридичних наук, професора, академіка-засновника НАПрНУ, першого Голови Конституційного Суду України

Леоніда Петровича Юзькова (м. Хмельницький, 28 лютого — 2 березня 2020 року). Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова. С. 213—216.

17. Линьов К.О. Інформаційне забезпечення державного управління та державної служби https://moodle.znu.edu.ua/pluginfile.php/719929/mod_resource/content/1/%D0%9D%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf

18. Ліпінська А. В. Інформаційно-комунікаційні технології в організації інформаційно-аналітичного забезпечення державного управління. Державне управління: удосконалення та розвиток. 2015. № 10. URL: http://www.dy.nayka.com.ua/pdf/10_2015/8.pdf.

19. Мінченков А.Ю. Сутність поняття інформаційна безпека в сучасній науці публічного управління. Наукові перспективи. 2024. №4(46). С. 296-307. DOI: [https://doi.org/10.52058/2708-7530-2024-4\(46\)-296-307](https://doi.org/10.52058/2708-7530-2024-4(46)-296-307)

20. Палагута С.С. Особливості інформаційного забезпечення підприємств і організацій. Миколаївський національний університет імені В.О. Сухомлинського.. 2-17. № 16. С. 418-421

21. Пантелейчук І. В. Теоретико-методологічні засади формування позитивного іміджу органів державної влади 25.00.01 – теорія та історія державного управління: дисертація на здобуття наукового ступеня доктора наук з державного управління. Київ, 2013. С. 309.

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

23. Підготовка державних службовців та посадових осіб місцевого самоврядування в Національній академії державного управління при Президентові України: інформаційний аспект: наук.-метод. матеріали /

уклад.: Т. А. Крушельницька, О. Б. Кукарін, Р. А. Науменко та ін. Київ : НАДУ, 2010. С. 48

24. Польська Т. Д. Відносини з громадськістю: соціально відповідальна комунікація в публічному управлінні. Вісник Національного університету цивільного захисту України: зб. наук. пр. (Серія «Державне управління»). Харків : Вид-во НУЦЗУ, 2018. Вип. 1 (8). 542 с

25. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

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

27. Про електронні документи та електронний документообіг: Закон України. № 851-IV від 31.12.2023. URL: http://www.e-ukraine.org.ua/index.php?mod=doc_obig

28. Про захист інформації в автоматизованих системах: Закон України. URL: <http://www.e-ukraine.org.ua/index.php?mod=2>

29. Про Концепцію Національну програму інформатизації: Закон України від 01.01.2022. № 75/98-ВР URL: <https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text>

30. Про затвердження завдань Національної програми інформатизації 2022-2024: Закон України № 2360-IX від 08.07.2022. URL: <https://zakon.rada.gov.ua/laws/show/2360-20#Text>

31. Про заходи щодо створення електронної інформаційної системи «Електронний уряд: Постанова Кабінету Міністрів України від 24.02.2003 №208. URL: <https://zakon.rada.gov.ua/laws/show/208-2003-%D0%BF#Text>

32. Про заходи щодо розвитку національної складової глобальної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні : Указ Президента України 928/2000 від 31.07.2000. URL: <https://zakon.rada.gov.ua/laws/show/928/2000#Text>.

33. Про правовий режим воєнного стану: Закон України від 27.07.2024. № 389-VIII URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text>
34. Про доступ до публічної інформації Закон України від 08.10.2023. № 2939-VI URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
35. Про основи кібербезпеки України: Закон України від 28.06.2024. № 2163-VIII URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
36. 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.
37. Синеокий О. В. Основи інформаційного права та законодавства у сфері високих технологій та ІТ-інновацій: навч. посіб. Харків: Право, 2011. – 591 с
38. Смотрич Д.В., Браїлко Л. Інформаційна безпека в умовах воєнного стану. Науковий вісник Ужгородського національного університету. 2023. С. 121-127.
39. Стадник В.Г. Інформаційне забезпечення формування аграрної політики в умовах гібридної війни. Актуальні проблеми економіки, управління та маркетингу в аграрному бізнесі: матеріали III Міжнародної наук.-практ. Інтернет-конференції, м. Дніпро, 03-04 жовтня 2024 р., Дніпро ДДАЕУ, 2024. С. 239-240.
40. Стадник В.Г. Інформаційна безпека в умовах воєнного стану. Розвиток форм і методів сучасного менеджменту в умовах глобалізації: Матеріали 12-ї Всеукраїнської наук.-практ. конф. – Дніпро, 8-9.11.2024: тези доповідей. – Дніпро: Поліграфічний відділ ДДАЕУ, 2024. С. 123-124.
41. Степанов В.Ю. Інформаційна безпека сучасного публічного управління. URL: <https://nuczu.edu.ua/images/topmenu/science/konferentsii/22-23.02.2017-1.pdf#page=123>
42. Сторожев Р. І. Кадровий механізм формування позитивного іміджу держави: дисертація на здобуття наукового ступеня кандидата наук з

державного управління: 25.00.02 – механізми державного управління. Київ, 2016. С. 282.

43. Про Стратегію інформаційної безпеки: Указ Президента України від 28.12.2021 №685/2021 . URL: <https://zakon.rada.gov.ua/laws/show/n0080525-21#Text>

44. Требик Л. Використання сучасних комп'ютерних технологій у роботі старост із громадськістю. Місцеве самоврядування. 2018. Липень. № 7. URL: <https://i.factor.ua/ukr/journals/ms/2018/july/issue-7/article-37831.html>.

45. Ушкало К.Ю. Інформаційний простір в умовах військового стану: безпековий аспект в Україні. Регіональні студії. 2023. С. 123-128 DOI <https://doi.org/10.32782/2663-6170/2023.35.20>

46. Філіпішина Л., Костик Є., Дзевелюк М. Публічне управління у сфері інформаційної безпеки (подолання суачсних загроз). Актуальні питання у сучасній науці. 2023. № 5 (11). С. 196-205

47. Шульга В.І. Сучасні підходи до трактування поняття інформаційна безпека. 2015.№ 4. URL: <http://www.economy.nayka.com.ua/?op=1&z=5514>

48. Business dictionary URL: <http://www.business-dictionary.com/definition/information.html>.

49. ISO/IEC 5127:2001 Information and documentation – Vocabulary URL: <https://www.iso.org/obp/ui/en/#iso:std:iso:5127:ed-1:v1:en:term:1.1.3.08>.

50. ISO/IEC 10746–2:2009 Information technology – Open distributed processing –Reference model: Foundations – Part 2 URL: <https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:10746:–2:ed-2:v1:en>

51. Horri A. Informology: A review of concepts and theories / A. Horri // Cultural Research Bureau. – 2003.

52. Semenets-Orlova, I., Halytska, N., Klochko, A., Skakalska, I., & Kosyuk, N. (2019). Information Exchange and Communication Infrastructure in the Public Sector. In CMiGIN (pp. 519–529).

53. Semenets-Orlova, I. A., & Kyselova, Y. Y. (2018). Multidimensional management contemporary: generation of social meanings for a new collective identities. *Публічне урядування*, (4), 264–273.

54. Wiener, N. (1983), "Cybernetics: Or Control and Communication in the Animal and the Machine