МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Інститут державного управління»

До захисту

Завідувач кафедри публічної політики
д.держ.упр., проф. В.Б. Дзюндзюк
_____
/Підпис/

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Кваліфікаційна робота на здобуття освітнього ступеня «магістр»
281 Публічне управління та адміністрування
28 Публічне управління та адміністрування

Виконавець
здобувач 2 курсу, групи ППГЗ-23_____ О.С. Донов

Науковий керівник _____ Р.Г. Соболь
к. держ. упр., доц.

Харків – 2024

ЗМІСТ

ВСТУП

Актуальність теми. Актуальність дослідження питання інформаційного забезпечення системи публічного управління в умовах гібридних загроз визначається кількома важливими аспектами, пов'язаними з розвитком інформаційних технологій, змінами в глобальній політиці та безпеці, а також новими викликами, які виникають внаслідок розвитку гібридних загроз. Гібридні загрози є складними, багатогранними і часто неочевидними, що ускладнює традиційні підходи до управління та реагування на них. Основними аспектами актуальності дослідження є: по-перше, зростаючий вплив інформаційних технологій на публічне управління. Інформаційні технології стали невід'ємною частиною системи публічного управління, надаючи нові можливості для збирання, аналізу та передачі даних. Однак, разом із цими можливостями зростають і ризики, пов'язані з інформаційними атаками, маніпуляціями з інформацією, кіберзагрозами тощо. По-друге, гібридні загрози як новий виклик для національної безпеки. Гібридні загрози включають комбінацію традиційних військових дій з невоєнними методами, такими як кібератаки, дезінформація, економічний тиск та використання соціальних мереж для маніпулювання громадською думкою. У таких умовах забезпечення достовірної та своєчасної інформації є критично важливим для ефективного управління кризовими ситуаціями та захисту національних інтересів. По-третє, необхідність адаптації до нових реалій. У зв'язку з розвитком гібридних загроз система публічного управління повинна бути здатною швидко адаптуватися до нових умов. Це включає оновлення стратегій і механізмів збору та обробки інформації, а також інтеграцію новітніх технологій у процеси державного управління. По-четверте, захист національної інформаційної безпеки. В умовах гібридної війни та глобальних інформаційних конфліктів інформаційна безпека стає одним з основних аспектів державної безпеки. Це включає захист критичної інфраструктури, інформаційних ресурсів і комунікаційних систем від

несанкціонованого доступу, атак та маніпуляцій з боку як внутрішніх, так і зовнішніх акторів. По-п’яте, роль національних інститутів у протидії інформаційним загрозам. Створення ефективних механізмів для збору, аналізу та передавання інформації, а також координація між різними державними установами та приватними структурами є важливою частиною національної стратегії безпеки. У цьому контексті важливим є розвиток інститутів, здатних проводити інформаційну розвідку, моніторинг загроз та ефективно реагувати на них. По-шосте, проблеми та виклики для організації інформаційного забезпечення. Основними проблемами є нестача кваліфікованих кадрів у сфері інформаційної безпеки, застарілість інфраструктури, а також недостатня координація між різними структурами державної влади, що можуть призводити до неефективного використання ресурсів і затримок у реагуванні на загрози.

Дослідженнями різних аспектів автоматизації управління і формування інформаційної інфраструктури займалися: В. Бакуменко, А. Голубицький, В. Дзюндзюк, Г. Климовицька, Т. Куценко, А. Никифоров, Я. Пущак, С. Чистов, О. Шевчук та інші.

Актуальність дослідження інформаційного забезпечення системи публічного управління в умовах гібридних загроз зумовлена необхідністю забезпечення ефективного, швидкого і надійного управління в умовах постійних змін у сфері безпеки та комунікацій. Це дослідження є важливим для розробки стратегій і рекомендацій, спрямованих на вдосконалення механізмів інформаційної безпеки та публічного управління в умовах сучасних загроз.

Мета магістерської роботи полягає в розробці науково-теоретичних засад і практичних рекомендацій щодо удосконалення інформаційного забезпечення системи публічного управління в умовах гібридних загроз.

Для досягнення мети в роботі були поставлені й вирішені *такі завдання:*

- обґрунтувати основи інформаційного забезпечення системи публічного управління в умовах гібридних загроз;
- встановити вплив комунікаційного менеджменту та маркетингу послуг на інформаційне забезпечення системи публічного управління в умовах гібридних загроз;
- проаналізувати стан застосування інформаційних технологій у побудові аналітично-інформаційного забезпечення функціонування публічних органів влади;
- дослідити сучасний стан впровадження інформаційного забезпечення інформаційних технологій у системі публічного управління міста Харкова в умовах гібридних загроз;
- запропонувати напрями впровадження сучасних інформаційних технологій у систему публічного управління в умовах гібридних загроз;
- розробити напрями застосування засобів мережі Internet у системі публічного управління в умовах гібридних загроз.

Об'єкт дослідження – процес інформатизації системи публічного управління.

Предметом дослідження є інформаційне забезпечення системи публічного управління в умовах гібридних загроз.

Методи дослідження. Методологічною основою дослідження є логіко-діалектичні методи наукового пізнання, системного аналізу, а також спеціальні методи, зокрема логічного узагальнення (дозволив сформувати структуру та зміст інформаційного забезпечення системи публічного управління в умовах гібридних загроз; розробити концептуальні підходи щодо впровадження в практику державної політики щодо інформаційного забезпечення системи публічного управління інформаційного забезпечення системи публічного управління в умовах гібридних загроз; порівняльного економічного аналізу (оцінити ефективність та тенденції формування та реалізації державної політики щодо інформаційного забезпечення системи

публічного управління в умовах гібридних загроз), статистичні методи та інші.

Інформаційну базу дослідження вкладають законодавчо-нормативні акти з питань реалізації та формування державної політики щодо інформаційного забезпечення системи публічного управління в умовах гібридних загроз, статистичні дані органів державної влади та інформаційно-аналітичних видань, статистична звітність вітчизняних і зарубіжних видань.

Практичне значення одержаних результатів полягає в тому, що сформульовані положення, методичні підходи та практичні рекомендації у сфері інформаційного забезпечення системи публічного управління в умовах гібридних загроз дозволяють підвищити ефективність роботи в державних органах виконавчої влади.

Основні результати роботи можуть бути використані в поточній роботі службовців та військових у Харківської області та при виробленні рекомендацій для удосконалення інформаційного забезпечення системи публічного управління в умовах гібридних загроз.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

1.1 Основи інформаційного забезпечення системи публічного управління в умовах гібридних загроз

Технологічні переміни, які чіпають інформаційне забезпечення, не могли не зворушити теж і публічне управління. Технологічні зміни, що стосуються інформаційного забезпечення, включають низку інновацій та розвитку в сферах обробки, зберігання, передачі та захисту інформації. Ось кілька основних напрямів, у яких відбуваються зміни. Цифровізація та автоматизація. Все більше організацій переходять до повної цифрової обробки даних, що дозволяє зменшити витрати, підвищити точність та ефективність управління інформацією. Використання штучного інтелекту (ШІ), роботизованих процесів автоматизації (RPA) та машинного навчання для автоматизації рутинних задач і прийняття рішень на основі даних [9].

Хмарні обчислення. Можливість зберігання та обробки даних у хмарах дозволяє зменшити витрати на інфраструктуру, збільшити гнучкість і доступність даних для різних користувачів у будь-якому місці.

Гібридні хмари. Підприємства використовують комбінацію приватних і публічних хмар для оптимізації витрат та безпеки. Великі дані та аналітика. Big Data: Зростання обсягів інформації веде до розвитку інструментів для зберігання, обробки та аналізу великих даних (Big Data), що дозволяє компаніям виявляти тренди, робити прогнози та оптимізувати бізнес-процеси.

Аналітика даних. Завдяки потужним аналітичним інструментам можна здійснювати глибокий аналіз даних, що допомагає приймати обґрунтовані управлінські рішення [6].

Інтернет речей (IoT). Поява пристроїв, підключених до Інтернету, значно розширює можливості збору та обробки даних. Це дозволяє збирати інформацію з різних джерел (сенсори, пристрої) в реальному часі для подальшого використання в аналітиці.

Блокчейн та дистрибутивні реєстри. Блокчейн. Технології розподілених реєстрів забезпечують високу надійність і безпеку зберігання інформації, що важливо для транзакцій та зберігання даних в умовах високої потреби в прозорості та довірі [20].

Захист інформації та кібербезпека.

З ростом кількості цифрових даних збільшується потреба в засобах захисту інформації. Кіберзагрози стають дедалі складнішими, тому організації впроваджують нові методи шифрування, багаторівневу аутентифікацію, а також інструменти для моніторингу і реагування на інциденти безпеки.

Захист персональних даних: Регуляції, такі як GDPR в Європейському Союзі, вимагають, щоб організації забезпечували належний захист персональних даних, що є важливою частиною інформаційного забезпечення.

Інтеграція та взаємодія інформаційних систем. Розвиток систем інтеграції (API, веб-сервіси) дозволяє з'єднувати різноманітні програмні рішення та забезпечувати безперебійну взаємодію між ними. Це важливо для забезпечення консистентності та ефективного використання даних в організаціях [40].

Штучний інтелект та машинне навчання. Використання ШІ для автоматичного аналізу та прогнозування, підтримка прийняття рішень, а також розвиток алгоритмів машинного навчання дозволяє ефективно обробляти великі обсяги даних і знаходити нові патерни, що допомагають у покращенні стратегій інформаційного забезпечення.

Перехід до 5G та нових мережевих технологій. Впровадження 5G та інших нових технологій зв'язку значно підвищує швидкість і якість передачі

інформації, що має великий вплив на обробку даних у реальному часі, відеоконференції, віртуальну реальність та інші інноваційні рішення.

Віртуалізація та контейнеризація. Віртуалізація дозволяє ефективніше використовувати ресурси серверів і знижувати витрати на апаратне забезпечення. Контейнеризація (наприклад, Docker) полегшує процеси розгортання і масштабування програмних рішень, підвищуючи гнучкість і ефективність IT-систем [44].

Адаптивні інтерфейси та користувацькі досвіди. Розвиток інтерфейсів, орієнтованих на користувача, забезпечує більш ефективну взаємодію з інформаційними системами. Модерні технології дозволяють персоналізувати досвід взаємодії з даними в залежності від уподобань користувача, що робить використання систем зручнішим.

Технологічні зміни в інформаційному забезпеченні дозволяють зростати ефективності організацій, знижувати витрати та створювати нові можливості для аналізу даних і автоматизації процесів. Вони забезпечують не тільки оптимізацію бізнес-процесів, а й покращення якості прийнятих рішень через більш точну і своєчасну інформацію.

Традиційна адміністративна модель управління розвивалась зі зміною технологій з рукописних на машинописні. Бюрократичні організації пристосовувались до таких змін та успішно функціонували за наявності паперового потоку, що проходив величезний ланцюг стадій створення, обробки, узгоджень та затвердження.

Інформаційне забезпечення системи публічного управління - це сукупність засобів, методів і технологій, які забезпечують ефективне збирання, обробку, збереження та використання інформації для підтримки процесів управління в державних органах та інших публічних структурах. Воно є основою для прийняття обґрунтованих рішень, аналізу ситуацій, планування діяльності, моніторингу та контролю [56].

Основні компоненти інформаційного забезпечення публічного управління:

Інформаційні ресурси:

– це дані та інформація, необхідні для прийняття рішень в управлінських процесах.

– включають статистичні дані, документи, звіти, аналітичні матеріали, бази даних тощо.

– важливими джерелами інформації є державні реєстри, інформаційні системи, дослідження, а також дані, що збираються з різних джерел через опитування, моніторинг тощо.

Інформаційні технології (ІТ):

– це програмне та апаратне забезпечення, яке дозволяє ефективно обробляти інформацію.

– включають різноманітні системи управління даними, аналітичні системи, інструменти для автоматизації документообігу, платформи для надання послуг громадянам тощо.

– ІТ допомагають в обробці великих обсягів інформації, в управлінні базами даних, інтеграції інформації між різними відомствами та органами влади.

Організаційні структури та процеси:

– організаційні механізми і процедури, які забезпечують обробку, передачу та використання інформації.

– включають встановлення політик і стандартів для зберігання і обміну інформацією між органами публічного управління, а також розподіл відповідальності за інформаційне забезпечення.

– організаційна структура включає в себе відділи, спеціалістів та комітети, які займаються питаннями інформаційної безпеки, управління базами даних, аналізу та використання інформації.

Інформаційні системи:

– інформаційні системи в публічному управлінні можуть бути різними: від простих систем обробки документів до складних комплексних

систем для моніторингу та управління ресурсами, планування соціальних програм чи надання послуг.

– прикладом таких систем є системи електронного урядування, які забезпечують електронне надання послуг громадянам та бізнесу, а також інтеграцію різних органів влади.

Інформаційна безпека:

– це забезпечення конфіденційності, цілісності, доступності та аутентичності інформації, що обробляється в системах публічного управління.

– включає захист від несанкціонованого доступу, помилок, кібератак і збоїв в інформаційних системах, а також заходи щодо забезпечення законності обробки персональних даних.

Аналіз та моніторинг:

– постійний аналіз та моніторинг інформації є необхідними для прийняття ефективних управлінських рішень.

– важливою частиною є створення аналітичних звітів та прогнозів, що базуються на зібраних даних, для розуміння поточної ситуації та планування майбутніх дій.

Прозорість та відкритість:

– система інформаційного забезпечення має забезпечувати прозорість діяльності органів публічного управління. Це включає відкритий доступ до інформації для громадян та бізнесу, що дозволяє їм брати участь у процесах прийняття рішень.

– важливими інструментами є відкриті дані, публікації про діяльність органів влади, звіти про бюджет та використання державних коштів.

Важливість інформаційного забезпечення:

Ефективність управління: Правильне і своєчасне використання інформації допомагає швидко реагувати на виклики та зміни в суспільстві,

забезпечує якісне управління ресурсами, оптимізацію процесів та прийняття точних рішень.

Підвищення доступності послуг: З ефективними інформаційними системами громадяни можуть легко отримувати публічні послуги без необхідності фізичної присутності в органах влади.

Прозорість та боротьба з корупцією: Застосування відкритих даних та автоматизованих процесів дозволяє зменшити можливості для корупційних зловживань, забезпечуючи доступність та підзвітність органів публічного управління.

Вдосконалення взаємодії між органами влади та громадянами: Завдяки інформаційним системам стає можливим здійснювати зворотний зв'язок, отримувати пропозиції та скарги від громадян, а також організовувати консультації та участь у процесах прийняття рішень [78].

Таким чином, інформаційне забезпечення системи публічного управління є важливим інструментом для розвитку сучасної демократичної держави, забезпечення її ефективності, прозорості та доступності для громадян.

Інформаційне забезпечення публічного управління — це система заходів, що охоплює організацію, збір, обробку, аналіз, зберігання та поширення інформації, необхідної для ефективного управління державними та місцевими органами влади [80]. Його основною метою є забезпечення відповідного рівня інформованості органів публічної влади для прийняття обґрунтованих управлінських рішень, а також забезпечення доступу громадян до інформації, що стосується їх прав і обов'язків.

Основні компоненти інформаційного забезпечення публічного управління:

Збір та обробка інформації:

– охоплює збирання даних з різних джерел (статистичні дані, соціологічні дослідження, звіти, документи тощо).

– обробка та аналіз цих даних для подальшого використання в управлінських процесах.

Інформаційні системи та технології:

– включають електронні системи, бази даних, програмне забезпечення для автоматизації збору, зберігання та аналізу даних.

– возвиток електронного урядування (e-Government) є важливою частиною, що дозволяє автоматизувати багато процесів в управлінні.

Моніторинг та оцінка:

– постійне відстеження та оцінка виконання управлінських рішень, щоб своєчасно коригувати стратегії та політики.

– використання показників ефективності та індикаторів для визначення результатів діяльності.

Комунікація та відкритість:

– забезпечення прозорості публічного управління, доступу громадян до державної інформації та можливості для зворотного зв’язку.

– інформація про бюджет, державні програми, законодавчі ініціативи та інші аспекти повинна бути доступною через офіційні вебсайти, публікації, консультації тощо.

Безпека інформації:

– забезпечення захисту інформаційних ресурсів від несанкціонованого доступу, втрати або пошкодження.

– використання сучасних технологій захисту інформації, кібербезпеки.

Залучення громадян і взаємодія з ними:

– інформаційне забезпечення публічного управління також включає збирання і аналіз громадської думки через опитування, електронні петиції, соціальні мережі тощо.

– спільне використання інформації органами влади і громадянами допомагає в побудові ефективних та орієнтованих на потреби громадян рішень.

Значення інформаційного забезпечення в публічному управлінні:

Покращення ефективності управління: Без належної інформації важко приймати обґрунтовані та своєчасні рішення. Інформаційне забезпечення дозволяє підвищити ефективність управлінських процесів, знизити рівень помилок та втрат.

Забезпечення прозорості та відкритості: Система інформаційного забезпечення забезпечує прозорість дій органів влади, що сприяє довірі громадян до публічних інститутів.

Створення основ для розвитку інновацій: Використання сучасних технологій (великий даних, штучний інтелект, блокчейн) дозволяє створювати нові можливості для розвитку державних послуг та покращення управлінських процесів [76].

Підвищення відповідальності органів влади: Постійний моніторинг і аналіз результатів діяльності дозволяє громадянам та контролюючим органам оцінювати ефективність роботи органів публічного управління.

Виклики та проблеми:

– інформаційна ізоляція між різними державними структурами може призводити до дублювання зусиль або недостатньої координації.

– необхідність забезпечення конфіденційності та захисту персональних даних при використанні великих обсягів інформації.

– неоднорідність інформаційної інфраструктури у різних регіонах або на рівнях управління може створювати бар'єри для ефективного функціонування системи.

Враховуючи всі ці аспекти, інформаційне забезпечення є ключовим фактором для розвитку сучасної держави, здатної адекватно реагувати на виклики часу та забезпечувати добробут своїх громадян [45].

Публічне управління в умовах гібридних загроз — це особливий тип управлінських викликів, що виникають у ситуаціях, коли традиційні форми війни і політичної боротьби поєднуються з використанням нетрадиційних методів впливу, таких як інформаційні маніпуляції, економічні санкції,

кібератаки, політичний тиск і інші елементи, що створюють загрозу для стабільності держави [73]. В умовах гібридних загроз органи публічного управління повинні адаптуватися до швидко змінюваного середовища та бути готовими до реакцій на широкий спектр нестандартних загроз.

Гібридні загрози — це комплексні, часто не традиційні форми агресії, які поєднують різні інструменти та методи впливу, щоб досягти стратегічних цілей, без застосування прямої військової сили або в умовах її мінімального використання [71]. Вони можуть включати політичні, економічні, інформаційні, кібернетичні, соціальні та інші методи, що дають змогу досягти ефекту на всіх рівнях — від державних органів до окремих громадян.

Основні характеристики гібридних загроз:

Мультидимензіональність: Гібридні загрози використовують одночасно кілька типів дій, таких як економічний тиск, інформаційні операції, кібератаки, дезінформацію, дипломатичні маніпуляції, а також пряме або непряме військове втручання.

Не визначеність джерела загрози: Вони можуть маскуватися під звичайні соціально-політичні конфлікти або навіть інтервенції з боку неурядових акторів, що ускладнює ідентифікацію та відповідь на загрозу.

Інформаційні та психологічні операції: Часто використовуються для маніпулювання громадською думкою, створення внутрішніх суперечностей або дестабілізації політичної ситуації в країні-цілі. Це може бути через фальшиві новини, пропаганду, кібератаки або інші форми впливу на інформаційний простір.

Використання нетрадиційних акторів: Гібридні загрози часто здійснюються не тільки державами, а й нелегітимними або проксі-акторами — такими як терористичні групи, злочинні угрупування, приватні військові компанії, волонтерські батальйони тощо [78].

Невизначеність у застосуванні сили: Можуть використовуватися часткові або обмежені військові дії, які не призводять до формальної війни, а скоріше створюють напруження та дестабілізують ситуацію на місцях.

Використання слабких місць суспільства: Гібридні загрози часто орієнтовані на вразливі місця — слабкі політичні структури, економічні проблеми, етнічні або релігійні суперечності, корупцію. Це дозволяє зменшити відкритий опір і досягти внутрішніх розколів.

Приклади гібридних загроз:

Російська агресія проти України (2014 року і надалі) — поєднання інформаційних операцій, кібератак, підтримки сепаратистських рухів та використання регулярних військ у вигляді "зелених чоловічків".

Кібернетичні атаки на державні структури та критичну інфраструктуру [78].

Інформаційна війна, де країни чи актори використовують соціальні мережі та медіа для поширення дезінформації та маніпуляцій.

Як протидіяти гібридним загрозам:

Інтегровані стратегії безпеки, що поєднують військові, інформаційні, економічні та дипломатичні засоби.

Посилення інформаційної безпеки, захист від кіберзагроз, моніторинг та нейтралізація дезінформації.

Міжнародна співпраця для протистояння загрозам та підтримки стабільності на глобальному рівні [80].

Гібридні загрози є важливою частиною сучасних конфліктів і стратегічної конкуренції, оскільки вони дозволяють досягати цілей без відкритого використання сили, що робить їх надзвичайно ефективними та важкими для відбиття за традиційними методами [72].

Характеристики гібридних загроз.

Комбінація традиційних і нетрадиційних методів: Гібридні загрози можуть включати військові операції, економічні санкції, інформаційні війни, кібернапади, підрив довіри до державних інститутів, спроби дестабілізації через внутрішні конфлікти тощо.

Невизначеність і невидимість: Гібридні загрози часто важко ідентифікувати на ранніх етапах, оскільки вони можуть проявлятися як низка локальних або непомітних подій, що з часом створюють серйозні наслідки.

Психологічний і інформаційний вплив: Інформаційні атаки, пропаганда, маніпуляції через соціальні медіа, фальшиві новини, а також створення розколів у суспільстві можуть мати глибокий ефект на стабільність країни без використання прямого насильства.

Міжнародна взаємодія: Гібридні загрози часто мають транснаціональний характер і включають не тільки дії одного суб'єкта (наприклад, іноземної держави чи нелегальних груп), а й вплив на міжнародні організації та альянси.

Публічне управління в умовах гібридних загроз.

У відповідь на ці нові виклики, публічне управління має адаптуватися до умов постійної загрози. Ось ключові елементи, які визначають ефективність управлінських структур у таких умовах:

Гнучкість і адаптивність органів управління.

Швидка реакція на зміну ситуації. В умовах гібридних загроз державні органи повинні бути готові до швидкого реагування на нові виклики. Це вимагає гнучкості у плануванні, прийнятті рішень та реалізації політик.

Міжвідомча координація. Ефективне управління вимагає тісної співпраці між різними державними відомствами (міністерствами, силовими структурами, дипломатичними службами, органами безпеки), а також залучення громадянського суспільства та приватного сектору.

Розвиток кіберзахисту і інформаційної безпеки.

Кібербезпека. У сучасних умовах гібридної війни кіберзагрози можуть мати вирішальне значення. Тому потрібно активно інвестувати в захист критичної інфраструктури від кібератак і розробляти ефективні стратегії для реагування на кібернапади.

Інформаційна війна. Захист інформаційного простору стає необхідністю. Органы влади повинні не тільки протидіяти фальшивим

новинам, пропаганді та маніпуляціям, але й активно створювати власний контент, який захищає національні інтереси та підтримує моральний дух громадян.

Посилення соціальної єдності і національної стійкості.

Створення єдиного фронту. Гібридні загрози часто використовують внутрішні розбіжності для дестабілізації ситуації. Важливо вжити заходів для зміцнення національної єдності та зниження ризиків соціальних конфліктів.

Громадянська готовність. Система публічного управління має працювати над підвищенням обізнаності населення щодо загроз та вміння адекватно реагувати на них. Це включає просвітницькі кампанії, тренінги та підготовку цивільного населення до кризових ситуацій.

Зміцнення законності та правової держави.

Підтримка верховенства права. В умовах гібридних загроз важливо забезпечити, щоб усі дії органів влади проводились на основі закону, з дотриманням прав людини та демократичних принципів. Відсутність правової визначеності може призвести до маніпуляцій з боку зовнішніх чи внутрішніх агресорів.

Інститут національної безпеки. Це може включати посилення інститутів, що відповідають за протидію тероризму, організованій злочинності, а також модернізацію армії та інших силових структур для швидкого реагування на загрози.

Залучення міжнародних партнерів та інститутів

Міжнародна підтримка. Гібридні загрози часто потребують міжнародного реагування. Важливо створювати ефективні механізми співпраці з міжнародними організаціями, такими як ООН, НАТО, ЄС та інші [59].

Дипломатичний тиск. В умовах гібридної війни важливо активно використовувати дипломатичні інструменти для нейтралізації зовнішніх загроз, включаючи економічні санкції, політичний тиск, а також формування альянсів.

Розвиток кризового управління.

Кризи управління в умовах гібридних загроз мають специфіку: необхідність оперативної та інтегрованої реакції на різноманітні загрози. Управлінські структури повинні мати чітко визначені плани дій у надзвичайних ситуаціях, які включають використання як традиційних, так і новітніх технологій.

Публічне управління в умовах гібридних загроз потребує системної адаптації до нових реалій глобальної безпеки. Ключовими аспектами є гнучкість, швидка реакція, інтеграція технологій кібербезпеки та інформаційної оборони, а також побудова ефективної внутрішньої та зовнішньої комунікації. Водночас важливо зберігати стабільність демократичних інститутів, захищати права і свободи громадян, підтримувати національну єдність і співпрацювати на міжнародному рівні.

1.2 Вплив комунікаційного менеджменту та маркетингу послуг на інформаційне забезпечення системи публічного управління в умовах гібридних загроз

На зараз фігурує кілька визнаних теоретичних моделей маркетингу послуг, будівниками яких є такі популярні учені, як М. Бітнер, Л. Беррі, Е. Гаммессон, К. Гренроос, Л. Ейгліє, В. Зейтхамл, Ф. Котлер, Е. Лангеард, А. Парасураман, Д. Ратмел [11, с. 91–95; 58, с. 3–7].

Маркетинг послуг — це процес просування і продажу нематеріальних товарів, які надаються клієнтам для задоволення їхніх потреб або вирішення конкретних проблем. Це важлива складова маркетингової стратегії будь-якої компанії, яка займається наданням послуг: від консалтингових компаній до сфер обслуговування, таких як готелі, ресторани, фінансові послуги тощо.

Ось кілька основних аспектів маркетингу послуг:

Нематеріальність. Послуги не можна побачити або відчути до того, як вони будуть надані, тому важливо створювати довіру та ясність для клієнта. Це можна зробити через відгуки, демонстрації або гарантії якості послуги.

Невід'ємність. Виробництво і споживання послуги часто відбувається одночасно, тобто, клієнт і постачальник взаємодіють під час надання послуги. Це створює важливість для кваліфікації і досвіду працівників компанії, а також уваги до індивідуальних потреб кожного клієнта.

Змінність. Послуги можуть змінюватися в залежності від того, хто, коли і де їх надає. Це означає, що потрібно стандартизувати послугу настільки, наскільки це можливо, щоб гарантувати стабільну якість.

Незберігання. Послуги не можна зберігати чи запасати. Якщо послуга не була надана у визначений час, вона просто втрачена. Це ставить завдання щодо точності виконання замовлень і планування ресурсів [10].

Маркетингова стратегія послуг. Включає кілька етапів:

– ідентифікація цільової аудиторії: хто є вашим потенційним клієнтом? Визначення потреб і бажань цільової групи.

– брендинг і репутація: оскільки послуги нематеріальні, ваш бренд та репутація — це ваші основні активи. Створення іміджу компанії як надійного і професійного постачальника послуг має критичне значення.

– ціноутворення: ціни на послуги можуть бути значною мірою залежними від ринку, конкуренції, а також від рівня обслуговування. Розробка гнучкої цінової політики дозволяє задовольнити різні сегменти споживачів.

– комунікація та просування: використання різноманітних каналів — від традиційної реклами до цифрових маркетингових стратегій, таких як SEO, контекстна реклама, соціальні мережі.

– покращення клієнтського досвіду: важливо не тільки надавати послугу, але й зробити досвід клієнта позитивним. Це може включати оптимізацію процесів надання послуги, покращення обслуговування та підтримки клієнтів, а також збір відгуків.

Інструменти маркетингу послуг:

– особистий маркетинг: комунікація з клієнтом через прямий контакт, консультації, переговори.

– інтернет-маркетинг: SEO, контент-маркетинг, email-маркетинг, SMM.

– промоакції та спеціальні пропозиції: акції, знижки, бонуси для постійних клієнтів.

– реклама та PR: формування репутації через медіа, онлайн-огляди, публікації у профільних виданнях.

Виклики в маркетингу послуг:

– важкість у вимірюванні ефективності: немає фізичного товару, який можна виміряти чи відчути, тому важливо звертати увагу на зворотний зв'язок від клієнтів і забезпечення високого рівня задоволення.

– побудова довгострокових відносин з клієнтами: створення постійних, лояльних клієнтів є важливим елементом для бізнесу в секторі послуг.

Маркетинг послуг передбачає створення унікальних пропозицій і забезпечення високої якості взаємодії з клієнтами, що допомагає забезпечити стабільність і зростання компанії в умовах жорсткої конкуренції [31].

Найбільш популярними закордонними моделями маркетингу послуг є:

Існує кілька закордонних моделей маркетингу послуг, які набули широкої популярності та успіху завдяки своїй ефективності. Ці моделі спрямовані на адаптацію та вдосконалення процесів надання послуг для досягнення найкращих результатів у конкурентному середовищі. Ось деякі з найбільш популярних моделей маркетингу послуг:

Модель 7P (Service Marketing Mix)

Модель 7P була розширенням класичної моделі 4P (Product, Price, Place, Promotion) для маркетингу послуг. Вона включає додаткові три компоненти, що є критичними для маркетингу нематеріальних товарів:

– Product (Продукт): послуга, яку компанія надає.

– Price (Ціна): ціна, яку споживач платить за послугу.

– Place (Місце): канали розподілу послуг, включаючи як фізичні локації (якщо це необхідно), так і онлайн-платформи.

– Promotion (Просування): методи просування послуг на ринку.

– People (Люди): працівники, які надають послугу. У маркетингу послуг особливо важливі кваліфікація, комунікаційні навички та досвід персоналу.

– Process (Процес): процес надання послуги, що включає стандартизацію та управління взаємодією з клієнтом.

– Physical Evidence (Фізичні докази): матеріальні елементи, що підтверджують якість послуги, наприклад, брендовані матеріали, зовнішній вигляд закладу, сайти, рекламні матеріали.

Модель 7P широко застосовується в готельному бізнесі, ресторанах, медицині, фінансових послугах, освіті та інших галузях [69].

Модель SERVQUAL.

SERVQUAL — це метод, що розроблений для вимірювання якості послуг на основі порівняння очікувань клієнта та реального досвіду від отриманої послуги. Модель SERVQUAL включає п'ять основних вимірів якості:

– Tangibles (Матеріальність): фізичне оснащення, персонал, комунікаційні матеріали.

– Reliability (Надійність): здатність надавати послугу правильно та точно.

– Responsiveness (Чуйність): готовність персоналу допомогти клієнту та швидко реагувати на запити.

– Assurance (Гарантія): рівень впевненості, який викликає персонал (кваліфікація, досвід, професіоналізм).

– Empathy (Емпатія): персоналізація обслуговування та індивідуальний підхід до кожного клієнта.

Модель SERVQUAL активно використовується для оцінки рівня обслуговування в різних сферах послуг, таких як готелі, ресторанний бізнес, банківські послуги, медичні установи.

Модель GAPS (Gap Model).

Gap Model (Модель прогалин) фокусується на виявленні різниць між сподіваннями клієнтів і фактичними стандартами послуг, що надаються підприємством. Ця модель складається з п’яти основних прогалин:

1. Gap 1: Прогалина між очікуваннями клієнтів і сприйняттям керівництвом компанії цих очікувань.

2. Gap 2: Прогалина між сприйняттям потреб клієнтів і фактичними специфікаціями послуг, які розробляються компанією.

3. Gap 3: Прогалина між специфікаціями послуг і фактичним виконанням цих послуг.

4. Gap 4: Прогалина між фактичним виконанням послуг і тим, як компанія комунікує свої послуги клієнтам.

5. Gap 5: Прогалина між сприйняттям клієнтом фактичної послуги та її очікуваннями.

Цей підхід дозволяє компаніям виявляти проблемні зони, які можуть призводити до незадоволення клієнтів, і вчасно коригувати свої стратегії надання послуг.

Модель "Ланцюг сервісу" (Service Chain Model).

Ця модель розглядає процес надання послуг як ланцюг, у якому кожна ланка — це окремий етап взаємодії з клієнтом [2]. Важливою особливістю є те, що задоволення кінцевого споживача залежить від якості обслуговування на кожному етапі ланцюга. Модель показує, що задоволені співробітники (внутрішні клієнти) надають кращі послуги зовнішнім клієнтам, тобто важливо створювати сприятливе середовище для працівників, щоб вони могли ефективно взаємодіяти з клієнтами.

Модель "Шість С"

Це ще одна модель, яка фокусується на шести важливих складових успішного маркетингу послуг:

– Customer (Клієнт): Потрібно розуміти потреби і бажання клієнтів.

– Cost (Ціна): Оцінка вартості послуги в очах клієнта.

– Convenience (Зручність): Як легко клієнти можуть отримати послугу.

– Communication (Комунікація): Як компанія комунікує зі своїми клієнтами.

– Consistency (Послідовність): Забезпечення стабільної якості послуг.

– Customer Satisfaction (Задоволення клієнтів): Головна мета маркетингу послуг — це створення задоволення у клієнтів.

Модель застосовується для створення стратегій, які сприяють не лише залученню нових клієнтів, але й утриманню існуючих.

Модель "Вартості послуг" (Service Value Model)

Ця модель акцентує увагу на створенні цінності для клієнтів.

Вона передбачає, що компанії повинні забезпечити клієнтів не тільки якісними послугами, але й сприяти їхньому досвіду, отриманому від процесу взаємодії з брендом.

Вона включає в себе такі аспекти, як персоналізація, інноваційність послуг та поліпшення взаємодії з клієнтом.

Ці моделі представляють собою різні підходи до маркетингу послуг, від оцінки якості до взаємодії з клієнтами і вдосконалення внутрішніх процесів. Кожна з них дає бізнесу можливість визначити слабкі місця в наданні послуг, покращити клієнтський досвід та досягти конкурентних переваг на ринку.

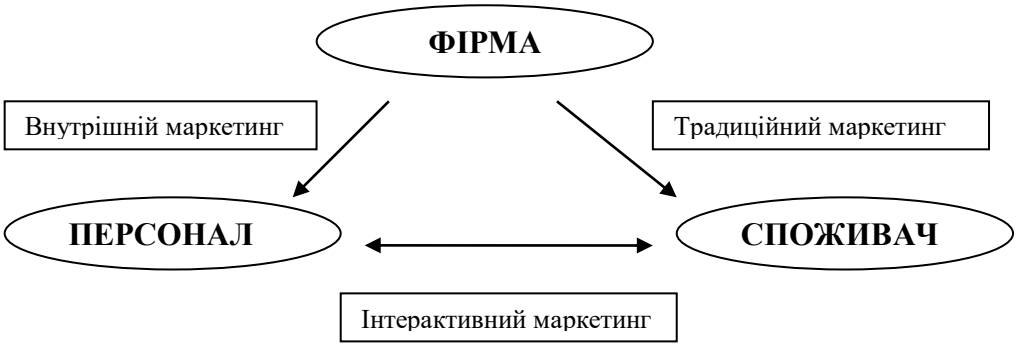

Рисунок 1.1 - Трикутникова модель маркетингу послуг Ф. Котлера

Комунікаційний менеджмент — це процес планування, організації, координації та контролю комунікаційних стратегій і заходів всередині організації та з зовнішнім середовищем 38. Він охоплює управління інформацією, забезпечення ефективного обміну даними, встановлення правильних комунікаційних каналів і створення зворотного зв'язку, що сприяє досягненню організаційних цілей.

Основні складові комунікаційного менеджменту:

1. Стратегічне планування комунікацій:

– розробка стратегії, яка відповідає загальним цілям компанії.

– визначення цільових аудиторій (внутрішніх та зовнішніх).

– формулювання основних повідомлень.

2. Інформаційні канали:

– вибір каналів для передачі інформації (засоби масової інформації, інтернет, соціальні мережі, корпоративні платформи тощо).

– визначення найефективніших методів комунікації в залежності від цільової аудиторії.

3. Управління репутацією та брендом:

– формування позитивного іміджу організації.

– реагування на кризові ситуації або скандали.

– просування бренду та створення довіри серед клієнтів і партнерів.

4. Зворотний зв'язок:

– збір і аналіз відгуків від різних аудиторій.

– використання зворотного зв'язку для поліпшення внутрішніх процесів і комунікаційної стратегії.

5. Криза комунікацій:

– планування заходів на випадок негативних ситуацій, криз або репутаційних загроз.

– залучення професіоналів для вирішення кризових комунікаційних ситуацій.

6. Міжнародна та міжкультурна комунікація:

– врахування культурних особливостей при веденні комунікацій у міжнародному контексті.

– адаптація стратегій для різних ринків та аудиторій.

7. Інтернал комунікації (внутрішні комунікації):

– управління інформацією та взаємодією всередині організації між співробітниками.

– забезпечення прозорості, залучення співробітників до корпоративної культури та місії компанії.

Загалом, ефективний комунікаційний менеджмент дозволяє створити позитивне середовище для розвитку організації, забезпечити її конкурентоспроможність, а також налагодити стійкі взаємини з ключовими стейкхолдерами [36].

Для того щоб ефективно управляти маркетингом у фірмі послуг, необхідно розвивати три стратегії спрямовані на ці три ланки. Стратегія традиційного маркетингу спрямована на ланку «державна установа-споживач» і пов’язана з питаннями ціноутворення, комунікацій і каналами поширення [39]. Стратегія внутрішнього маркетингу спрямована на ланку «державна установа-персонал» і пов’язана з мотивацією персоналу на якісне обслуговування споживачів. Нарешті, стратегія інтерактивного маркетингу спрямована на ланку «персонал-споживач» і пов’язана з контролем якості

надання послуги, що відбуває в процесі взаємодії персоналу й споживачів [41].

Особливість маркетингу послуг полягає в тому, що послуги є нематеріальними, непостійними та невіддільними від постачальника, що створює унікальні виклики для їх просування на ринку. Ось кілька ключових характеристик маркетингу послуг:

1. Нематеріальність: Послуги не можна побачити, потримати чи спробувати до того, як їх отримано. Це ускладнює споживачам прийняття рішення про покупку, оскільки вони не можуть оцінити якість до отримання послуги. Тому важливу роль відіграють репутація бренду, відгуки клієнтів і демонстрація якості через рекламні матеріали або кейс-стаді.

2. Невіддільність: У процесі надання послуги клієнт часто бере участь безпосередньо у її створенні (наприклад, у процесі навчання, лікування чи обслуговування). Це означає, що якість послуги залежить не лише від постачальника, але й від активності або поведінки клієнта.

3. Нестабільність (варіативність): Послуга може змінюватися залежно від часу, місця, співробітників або навіть настрію клієнта. Це робить стандартизацію та контроль якості складнішими порівняно з товарними продуктами. Для забезпечення стабільності часто використовують тренування персоналу і встановлення стандартів обслуговування.

4. Невідкладність (несхоронність): Послуги не можуть бути збережені чи перенесені на майбутнє. Якщо послугу не спожито в момент її надання, це може призвести до втрати (наприклад, в готелях чи авіаперевезеннях, де не використаний номер або місце на рейсі втрачається без компенсації).

5. Взаємодія з клієнтом: Оскільки послуги часто надаються безпосередньо через взаємодію з клієнтом, значну роль відіграє досвід обслуговування та комунікація. Якість персонального сервісу може впливати на загальне сприйняття бренду.

Роль маркетингу послуг та комунікаційного менеджменту в інформаційному забезпеченні системи публічного управління є надзвичайно

важливою для ефективного функціонування державних органів, покращення взаємодії з громадянами та забезпечення прозорості державних процесів [32]. Ось кілька основних аспектів цієї ролі:

1. Маркетинг послуг у публічному управлінні

Маркетинг послуг у контексті публічного управління включає в себе стратегічне планування та впровадження заходів, що дозволяють органам влади краще взаємодіяти з громадянами, надавати послуги на найвищому рівні та забезпечувати їх доступність. Це включає:

– Аналіз потреб громадян: Для ефективного управління необхідно зрозуміти, які саме послуги потрібні, в який спосіб вони повинні бути надані, та яким чином їх споживачі (громадяни) можуть отримати зручний і швидкий доступ до цих послуг.

– Покращення якості послуг: Застосування принципів маркетингу дозволяє знижувати бар'єри доступу до державних послуг, забезпечувати їх високу якість та результативність.

– Прозорість і довіра: Ефективний маркетинг допомагає формувати позитивний імідж органів публічного управління та збільшувати довіру громадян до державних інститутів, підвищуючи їхню участь у суспільних процесах.

2. Комунікаційний менеджмент у публічному управлінні

Комунікаційний менеджмент є важливою частиною сучасного публічного управління, адже він визначає ефективність внутрішньої та зовнішньої комунікації в органах влади. Це включає в себе:

– Інформаційна підтримка прийняття рішень: Чітке і оперативне донесення інформації до всіх учасників процесу управління дозволяє ухвалювати більш обґрунтовані та ефективні рішення. Розробка ефективних стратегій комунікації допомагає сприяти чітким і скоординованим діям на всіх рівнях публічного управління.

– Комунікація з громадянами: Однією з ключових задач є формування та підтримка двостороннього діалогу між державними органами

та громадянами. Це включає використання соціальних медіа, офіційних вебсайтів, мобільних додатків та інших каналів для інформування про державні ініціативи, зміни в законодавстві, новини та важливі події.

– Підвищення обізнаності громадян: Задля забезпечення громадської підтримки та участі в управлінських процесах важливо не лише передавати інформацію, а й сприяти підвищенню рівня обізнаності громадян про їхні права та обов’язки.

3. Інформаційне забезпечення публічного управління

Інформація є важливим ресурсом для будь-якої організації, а для публічного управління вона є критично важливою для забезпечення ефективності функціонування державних структур [54]. Комунікаційний менеджмент та маркетинг допомагають створювати структури, які забезпечують збирання, обробку та надання цієї інформації:

– Доступність та прозорість інформації: Важливо забезпечити громадянам вільний доступ до інформації про діяльність державних органів, проекти, програми, бюджетні витрати та інші важливі аспекти, що підвищує рівень довіри до держави та сприяє громадському контролю.

– Цифровізація та автоматизація процесів: Використання сучасних технологій для збору, зберігання та передачі інформації значно спрощує взаємодію між органами влади та громадянами. Впровадження електронних платформ для подачі заяв, запитів, скарг дозволяє швидше отримати відповідь на звернення, а також зменшити корупційні ризики.

– Аналітика та прогнозування: Застосування аналітичних інструментів дозволяє органам публічного управління краще прогнозувати потреби та вимоги громадян, аналізувати ефективність політик і коригувати стратегії на основі зібраних даних.

4. Проблеми та виклики

– Низький рівень довіри до державних органів: Високий рівень корупції, недостатня прозорість та інші проблеми можуть перешкоджати

ефективному використанню маркетингу та комунікаційного менеджменту в публічному управлінні.

– Недостатнє фінансування: Бюджетні обмеження можуть бути суттєвою перешкодою для впровадження нових технологій і стратегій комунікацій, зокрема для створення ефективних інформаційних систем.

– Технічні проблеми: Необхідність постійного оновлення та вдосконалення інформаційних систем, створення зручних і доступних платформ для громадян.

5. Перспективи розвитку

– Інтеграція нових технологій: Впровадження інструментів штучного інтелекту, великих даних (big data), машинного навчання для підвищення ефективності аналізу потреб громадян і адаптації послуг.

– Ефективне використання соціальних медіа та мобільних додатків: Розвиток комунікації через цифрові платформи дозволяє швидше і зручніше отримувати інформацію від державних органів, зменшуючи відстань між владою та громадянами.

– Інклюзивність та персоналізація послуг: Використання індивідуальних підходів до громадян, створення персоналізованих пропозицій і послуг для різних груп населення.

Отже, маркетинг послуг та комунікаційний менеджмент є важливими інструментами для забезпечення ефективної роботи публічного управління, що, в свою чергу, має безпосередній вплив на якість життя громадян, розвиток державних інститутів та підвищення рівня довіри до влади.

1.3 Сучасні технології у комунікаційному забезпеченні публічного управління

Інформатизація — це процес впровадження інформаційних технологій і систем у різні сфери діяльності людини, який сприяє розвитку суспільства, економіки, науки, освіти та інших галузей. Вона охоплює широкий спектр

змін, від автоматизації виробничих процесів до модернізації освітніх і управлінських систем [**Ошибка! Источник ссылки не найден.**, с. 11].

Інформатизація передбачає:

1. Збір, обробка та збереження інформації — впровадження комп'ютерних та інформаційних технологій для швидкого збору та обробки даних.

2. Автоматизація процесів — використання програмного забезпечення та апаратних засобів для автоматичного виконання завдань, що раніше виконувались вручну.

3. Доступ до інформації — створення інформаційних ресурсів, які забезпечують доступ до важливої інформації через мережі (зокрема Інтернет).

4. Розвиток інфраструктури інформаційних технологій — будівництво та модернізація технічної інфраструктури для підтримки інформаційних систем, таких як дата-центри, сервери, мережі передачі даних.

5. Освіта та підготовка кадрів — розвиток навичок та знань у галузі інформаційних технологій серед різних груп населення.

Інформатизація має важливе значення для підвищення ефективності управлінських рішень. Так, інформатизація дійсно має важливе значення для підвищення ефективності управлінських рішень. Вона передбачає інтеграцію сучасних інформаційних технологій в процеси управління, що дозволяє організаціям швидше та точніше реагувати на зміни, зменшувати ризики і приймати більш обґрунтовані рішення.

Основні переваги інформатизації для управлінських рішень включають:

1. Швидкий доступ до інформації: Інформаційні системи дозволяють зберігати та обробляти величезні обсяги даних, що забезпечує доступ до актуальної інформації в режимі реального часу. Це дає змогу керівникам швидко реагувати на зміни в зовнішньому та внутрішньому середовищі.

2. Покращення аналітики та прогнозування: Інструменти для аналізу даних, такі як бізнес-аналіз, моделювання та прогнозування, допомагають керівникам краще оцінювати потенційні наслідки різних рішень і вибирати оптимальний шлях дій.

3. Автоматизація процесів: Інформатизація дозволяє автоматизувати багато рутинних задач, таких як облік, звітність, планування, що в свою чергу знижує витрати часу та мінімізує помилки, забезпечуючи більшу точність та ефективність.

4. Поліпшення комунікації та співпраці: Використання інформаційних технологій покращує обмін інформацією між різними рівнями управління та співробітниками організації. Це сприяє більш ефективному вирішенню проблем, швидкому реагуванню на запити та зміни в умовах роботи.

5. Прийняття обґрунтованих рішень: Використання інформаційних систем допомагає обробляти великі обсяги даних, що дозволяє приймати рішення на основі точних і перевірених фактів, а не припущень або інтуїції.

Таким чином, інформатизація є важливим інструментом для підвищення ефективності управлінських рішень і загальної продуктивності організації.

Так, дійсно, сучасний світ переживає глибокі трансформації, і роль людини в ньому змінюється відповідно до цих змін [41]. Технологічні досягнення, глобалізація, зміни в економічних, соціальних і культурних сферах — усе це створює нові умови для життя та діяльності людей. Розглянемо, як трансформується роль людини у сучасному світі:

Розвиток автоматизації, роботизації та штучного інтелекту змінює характер праці [40]. Багато традиційних професій можуть бути замінені технологіями, що звільняє людей від рутинної та фізичної праці, але водночас вимагає від них нових навичок та адаптації до нових умов. Роль людини зміщується в бік більш творчих, аналітичних та стратегічних завдань. Замість виконання однотипних операцій люди починають більше працювати з даними, приймати складні рішення та інновувати.

Перехід до цифрової економіки та розвиток нових бізнес-моделей, таких як економіка спільного споживання (sharing economy), зміщує акценти на ефективність використання ресурсів, інновації та створення доданої вартості через знання та креативність. У такому світі людина повинна постійно адаптуватися до нових умов, здобувати нові навички і бути відкритою до змін [49].

Технології змінюють спосіб комунікації, формуючи нові соціальні мережі та платформи для взаємодії. Це створює нові можливості для розвитку особистості, для навчання та самовираження, але також породжує нові виклики, такі як проблема цифрового відчуження, надмірної залежності від технологій або етичні питання, пов'язані з приватністю та безпекою даних [66].

Сучасний світ стає дедалі більш взаємозалежним. Глобалізація розширює можливості для міжкультурної взаємодії, але водночас ставить нові вимоги до людей, такі як здатність адаптуватися до різних культурних контекстів, працювати в міжнародних командах і вирішувати глобальні проблеми (зміни клімату, бідність, пандемії). Людина стає все більш частиною глобального суспільства, де її роль полягає не лише у вирішенні локальних завдань, але й у знаходженні рішень, які матимуть позитивний вплив на весь світ.

У світі, що змінюється, постійно зростає значення знань та навичок для особистісного і професійного розвитку. Освіта стає не просто етапом життя, а постійним процесом, впродовж якого людина повинна вчитися, адаптуватися і розвиватися, щоб не відставати від швидких змін. Зараз важливо вміти критично мислити, адаптуватися до нових технологій і працювати в умовах невизначеності [42].

З розвитком нових технологій, таких як штучний інтелект, генна інженерія чи біотехнології, постає питання етики і моралі. Людина, як основний агент цих змін, повинна брати на себе відповідальність за їх наслідки, визначати межі використання технологій і забезпечувати їх етичне

застосування. Роль людини полягає не тільки в тому, щоб створювати нові можливості, але й у тому, щоб вирішувати, як ці можливості застосовувати з максимальною користю для суспільства.

В умовах глобальних змін важливе значення має пошук ідентичності в цифровому середовищі. Людина все більше живе в онлайні, де її особистість може бути представлена через різноманітні соціальні платформи. Це ставить нові питання про те, як зберігати свою автентичність, балансуючи між реальним і віртуальним світом [47].

Однією з ключових проблем сучасності є зміни клімату та екологічна криза. У цьому контексті роль людини змінюється: вона стає не лише споживачем природних ресурсів, але й відповідальним за сталий розвиток, охорону довкілля та трансформацію економічних моделей до більш екологічно безпечних. Людина повинна ставати активним учасником глобальних ініціатив збереження планети для майбутніх поколінь.

Трансформація світу супроводжується глибокими змінами в ролі людини. Вона повинна не тільки адаптуватися до нових умов, а й активно впливати на ці зміни. Знання, адаптивність, етична відповідальність та здатність до інновацій — ось ключові характеристики, які визначатимуть роль людини в майбутньому.

Сьогодні для України гострою залишається проблема розвитку Е-демократії [60].

Е-демократія, зазначає Стівен Кліфт, являє собою використання інформації і технологій зв’язку і стратегій демократичними акторами (державними інституціями, парламентарями, медіа, політичними організаціями, громадянами/виборцями) у межах політичного й управлінського процесів локальних суспільств, країни в цілому і на міжнародній арені.

Е-демократія (електронна демократія) — це використання інформаційних і комунікаційних технологій для покращення та розвитку демократії, зокрема для посилення участі громадян у процесах ухвалення

політичних рішень, забезпечення прозорості та підзвітності урядів, а також для полегшення доступу до державних послуг і посилення демократичної участі [7].

Основні принципи і елементи е-демократії:

Цифрова участь громадян

Е-демократія дозволяє громадянам активно брати участь у політичних процесах через інтернет. Це може включати:

– Електронні петиції: можливість подавати петиції або звернення до урядів через онлайн-платформи.

– Онлайн-голосування: можливість голосувати в виборах або референдумах через електронні платформи, що знижує бар'єри для участі в демократичних процесах.

– Форумні обговорення та опитування: громадяни можуть брати участь у обговореннях важливих питань, залишати відгуки або брати участь в онлайн-опитуваннях, що дозволяє урядам отримувати зворотний зв'язок від суспільства.

Прозорість і підзвітність

– Використання технологій може значно збільшити прозорість державних органів і процесів. Це включає:

– Доступ до державної інформації: онлайн-доступ до бюджету, законопроектів, рішень, зустрічей урядових органів.

– Інтерактивні платформи: сайти, де можна слідкувати за виконанням обіцянок політиків, результатами голосувань, діяльністю органів влади.

– Онлайн-платформи для моніторингу: інструменти, що дозволяють громадянам оцінювати ефективність урядів і органів влади.

Мобільність і доступність.

Інтернет-технології роблять політичні процеси доступними для широких верств населення:

– Доступ до інформації через мобільні додатки: платформи, через які люди можуть отримувати актуальну політичну інформацію, брати участь в опитуваннях чи подати петицію.

– Можливість голосування через мобільні пристрої: розвиток технологій для безпечного онлайн-голосування дозволяє громадянам брати участь у виборах з будь-якого місця, що є важливим для людей з обмеженими можливостями або тих, хто перебуває за кордоном.

Технології для взаємодії урядів з громадянами [30].

Інтернет може забезпечити прямий зв'язок між урядами і громадянами, що дає змогу:

– Платформи для електронного уряду: уряди можуть надавати громадянам можливість подавати податкові декларації, отримувати послуги (наприклад, реєстрація бізнесу, видача документів тощо) онлайн.

– Цифрові форуми для обговорення політики: забезпечення можливості для громадян обговорювати законопроекти або ініціативи через інтернет.

Цифрове голосування та вибори

В е-демократії важливе місце займають технології для організації електронних виборів або голосувань:

– Безпечне онлайн-голосування: застосування криптографії та інших технологій для забезпечення конфіденційності і цілісності голосів виборців.

– Зменшення бар'єрів для участі: можливість голосувати з будь-якої точки світу за допомогою мобільних пристроїв або комп'ютерів.

Соціальні медіа як інструмент політичної комунікації

Соціальні медіа стали потужним інструментом для політичних кампаній, а також для зв'язку громадян із урядовими структурами:

– Платформи для обговорення політичних питань: соціальні медіа дозволяють громадянам активно висловлювати свої думки щодо поточних подій, законодавчих ініціатив та політичних кампаній.

– Налагодження зв'язку з політиками: через соціальні медіа політики можуть безпосередньо комунікувати з громадянами, а громадяни — ставити запитання або висловлювати свою думку.

7. Підвищення ефективності законодавчого процесу

Використання цифрових технологій може зробити законодавчі процеси більш відкритими і ефективними:

– Цифрові платформи для обговорення законопроектів: громадяни можуть бути залучені до розробки нових законів через онлайн-платформи, де можна вносити пропозиції або голосувати за певні поправки.

– Автоматизація законодавчих процедур: використання інструментів для моніторингу та автоматизації процесів прийняття законів може значно зменшити час, необхідний для ухвалення рішень.

Виклики та ризики е-демократії:

1. Цифровий розрив: не всі громадяни мають доступ до інтернету або навички використання новітніх технологій, що може створювати нерівні можливості для участі у політичному процесі.

2. Кібербезпека: захист даних та забезпечення безпеки онлайн-голосувань і комунікацій — це серйозна проблема для е-демократії.

3. Маніпуляції та фейки: уразливість до маніпуляцій через соціальні медіа та інші онлайн-ресурси може загрожувати політичним процесам, адже дезінформація може швидко поширюватися через цифрові канали.

4. Конфіденційність і приватність: збереження приватності громадян під час участі в цифрових політичних процесах є важливим завданням, особливо в контексті збору персональних даних.

Е-демократія — це потужний інструмент для підвищення ефективності демократії, що надає громадянам нові можливості для участі в політичному житті, забезпечує більшу прозорість і доступність урядів [30]. Однак для її успішної реалізації необхідно враховувати технічні, соціальні та етичні аспекти, аби забезпечити рівні можливості для всіх громадян і зберегти безпеку та конфіденційність в умовах цифрового світу.

Однією з основних ідей е-демократії є те, що сучасні технології — такі як Інтернет, мобільний зв'язок та інші цифрові інструменти — значно розширюють можливості для громадян брати участь у політичних процесах, що робить демократичні механізми більш доступними та ефективними [77].

Технології дозволяють громадянам отримувати інформацію в реальному часі, що значно покращує їх обізнаність про політичні процеси, законодавчі ініціативи та поточні події. Завдяки цьому люди можуть зробити більш обґрунтовані та свідомі рішення щодо своєї участі в демократичних процесах. Онлайн-ресурси, платформи для новин, цифрові урядові сайти — все це дає можливість громадянам швидко отримувати інформацію та брати участь у дискусіях [79].

Мобільні телефони, смартфони і мобільний Інтернет відкривають нові можливості для участі громадян у політичному житті. Наприклад, люди можуть голосувати онлайн, підписувати петиції, брати участь у опитуваннях або долучатися до політичних кампаній через мобільні додатки [81]. Мобільні платформи дають змогу легко підтримувати зв'язок з політиками або громадськими організаціями та оперативно реагувати на важливі події.

Технології дозволяють не лише пасивно спостерігати за політичними процесами, а й активно впливати на них. Партисипаторні форми демократії, що включають пряме залучення громадян до ухвалення рішень, стали можливими завдяки інтернету та мобільним технологіям [75]. Такі інструменти, як:

– електронні петиції — дозволяють громадянам ініціювати важливі соціальні чи політичні зміни, звертаючи увагу на проблеми, що потребують вирішення.

– онлайн-консультації — платформи для обговорення законопроектів, де громадяни можуть подати свої зауваження або пропозиції до нових законів.

– пряме голосування — можливість здійснювати голосування через інтернет або мобільні додатки дає громадянам більше свободи в участі в референдумах, виборах чи інших політичних ініціативах.

Однією з важливих переваг е-демократії є зниження бар'єрів для участі. Традиційно участь у політичному житті обмежувалася різними факторами — часом, фізичними перешкодами, доступом до інформації, відсутністю можливості прямого контакту з політиками. Завдяки сучасним технологіям ці бар'єри значно зменшуються:

– громадяни можуть легко долучатися до політичних процесів, не виходячи з дому.

– люди з обмеженими можливостями або ті, хто проживає в віддалених регіонах, також можуть брати активну участь у демократії через онлайн-ресурси.

Інтернет, соціальні медіа та мобільні технології дозволяють громадянам безпосередньо взаємодіяти з політиками. Через соцмережі та інші платформи люди можуть ставити питання політикам, висловлювати свою думку щодо їхньої діяльності або реагувати на їхні заяви та пропозиції. Ця комунікація робить політиків більш доступними для виборців, а громадян — більш залученими до політичних процесів.

Технології змінюють традиційні форми демократії, зокрема, представницьку демократію, в бік більш партисипаторних і прямих форм участі. Вони дозволяють громадянам безпосередньо брати участь у прийнятті рішень через механізми, які раніше були недоступні або складні для реалізації [62].

Представницька демократія, у якій громадяни обирають своїх представників для ухвалення рішень, залишається основою політичних систем багатьох країн. Проте завдяки е-демократії з'являються нові можливості для громадян впливати на процеси прийняття рішень і на самих представників.

Пряма демократія — це можливість громадян безпосередньо впливати на рішення через референдуми, голосування або інші форми прямої участі. Завдяки технологіям, як електронне голосування, це стає більш доступним і зручним для широкого кола людей.

Приклади успішного використання е-демократії:

Естонія є одним із лідерів у сфері е-демократії. Вона впровадила систему електронного голосування на виборах, систему е-ідентифікації та електронних підписів, що дозволяє громадянам взаємодіяти з урядом швидко та безпечно.

Ісландія використовувала онлайн-платформи для залучення громадян до процесу створення нової конституції, дозволяючи їм вносити зміни та пропозиції через інтернет.

Індія активно використовує мобільні платформи для проведення опитувань та збору думок громадян щодо важливих політичних рішень.

Технології дійсно трансформують демократію, роблячи її більш інклюзивною, прозорою і доступною для більшої кількості людей. Це не лише підвищує рівень участі громадян у політичному житті, а й сприяє розвитку більш ефективних і адаптивних політичних систем, що краще відповідають потребам сучасного суспільства [57].

Інформаційні технології (ІТ) відіграють важливу роль у розвитку публічного управління, зокрема в забезпеченні ефективних комунікацій між державними органами, громадянами та іншими зацікавленими сторонами. З впровадженням новітніх технологій комунікація стає більш прозорою, доступною та зручнішою, що сприяє покращенню управлінських процесів і взаємодії між різними рівнями державної влади.

Покращення комунікацій між органами влади.

Інформаційні технології дозволяють державним органам обмінюватися даними в реальному часі, що сприяє швидкому ухваленню рішень та зменшенню бюрократичних затримок. Зокрема:

– використання електронних документів і систем обміну інформацією між відомствами дозволяє спростити процеси реєстрації, погодження та зберігання документів.

– впровадження електронних архівів забезпечує централізований доступ до важливої інформації, що допомагає у прийнятті обґрунтованих рішень.

Електронне урядування (e-Government)

Електронне урядування — це впровадження інформаційних технологій у діяльність державних органів для покращення комунікації з громадянами та забезпечення прозорості. За допомогою електронних платформ громадяни можуть:

– звертатися до органів влади через онлайн-сервіси для отримання послуг.

– отримувати актуальну інформацію про діяльність органів влади, зміни в законодавстві, оголошення конкурсів і тендерів.

– брати участь у електронних голосуваннях та петиціях.

Забезпечення прозорості та підзвітності.

Інформаційні технології сприяють підвищенню рівня прозорості в публічному управлінні:

– платформи для публікації бюджету, звітів та іншої важливої інформації допомагають громадянам та громадським організаціям відстежувати, як використовуються державні кошти.

– системи моніторингу та звітності дозволяють контролюючим органам швидше виявляти порушення та зловживання.

Залучення громадян до процесу управління.

ІТ забезпечують більше можливостей для участі громадян у процесах публічного управління:

– через онлайн-консультації, опитування та форуми громадяни можуть висловлювати свої думки щодо важливих управлінських рішень.

– електронні петиції дозволяють громадянам ініціювати зміни в законодавстві або в діяльності органів влади.

Безпека та конфіденційність даних.

Впровадження ІТ у публічне управління вимагає особливої уваги до питань безпеки та захисту персональних даних. Застосування сучасних технологій шифрування, а також систем захисту від кібератак забезпечують конфіденційність обміну інформацією, що є необхідним для підтримки довіри між громадянами та органами влади.

Аналіз даних і прийняття рішень.

ІТ дозволяють здійснювати глибокий аналіз великих обсягів даних, що збираються в процесі публічного управління. Використання аналітичних інструментів дозволяє:

– виявляти тренди та проблеми, що потребують втручання.

– прогнозувати розвиток ситуацій на основі статистичних даних.

– оптимізувати процеси прийняття рішень через системи підтримки прийняття рішень (DSS).

Мобільні технології та соціальні мережі

Використання мобільних додатків і соціальних мереж також сприяє поліпшенню комунікацій між громадянами та органами влади:

– мобільні додатки дозволяють громадянам отримувати актуальну інформацію, подавати заявки та звернення в будь-який час.

– соціальні мережі дають можливість органам влади безпосередньо комунікувати з громадянами, проводити інформаційні кампанії та отримувати зворотний зв'язок.

Виклики та перспективи розвитку.

Хоча інформаційні технології значно покращують комунікації в публічному управлінні, є і ряд викликів:

– низький рівень цифрової грамотності у деяких категорій населення може обмежити доступ до електронних послуг.

– проблеми безпеки та кіберзахисту вимагають постійного удосконалення заходів для захисту даних.

– необхідність інтеграції різних інформаційних систем між державними органами, що потребує значних інвестицій у модернізацію інфраструктури.

Інформаційні технології є потужним інструментом, що дозволяє значно підвищити ефективність комунікацій у публічному управлінні. Вони сприяють покращенню доступності та прозорості державних послуг, активізації громадської участі в управлінських процесах і зниженню корупційних ризиків. Проте, для повного реалізування потенціалу ІТ у публічному управлінні необхідно вирішити ряд технічних, організаційних і правових питань.

РОЗДІЛ 2
АНАЛІЗ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

2.1 Застосування інформаційних технологій у побудові аналітично-інформаційного забезпечення функціонування публічних органів влади

Система публічного управління є важливою складовою інфраструктури будь-якої країни, забезпечуючи ефективну організацію державних органів, їх взаємодію з громадянами, а також реалізацію політичних, соціальних і економічних рішень. У сучасних умовах ця система стикається з численними викликами, зокрема з гібридними загрозами, які включають не лише традиційні військові методи, а й інформаційні, кібернетичні та психологічні операції, які спрямовані на дестабілізацію держави.

Гібридні загрози можуть проявлятися через маніпуляцію інформацією, пропаганду, кібератаки, економічний тиск тощо. Для успішного протистояння таким викликам важливою умовою є розробка і реалізація ефективної стратегії інформаційного забезпечення в рамках публічного управління [40].

Інформаційне забезпечення публічного управління — це сукупність заходів, спрямованих на ефективне забезпечення органів державної влади та місцевого самоврядування необхідною інформацією для прийняття обґрунтованих рішень у різних сферах діяльності [33].

Воно включає в себе:

– збір, обробку та аналіз інформації,

– формування інформаційних потоків для підтримки прийняття рішень,

– забезпечення доступу громадян до публічної інформації.

Сучасні інформаційні технології дозволяють створювати ефективні механізми управління, автоматизувати процеси прийняття рішень, а також забезпечити прозорість і відкритість для громадян.

Гібридні загрози є складним поєднанням традиційних військових і новітніх інформаційних технологій, спрямованих на досягнення стратегічних цілей без застосування відкритої військової сили. У контексті публічного управління вони включають:

– інформаційні війни: поширення дезінформації, маніпуляція громадською думкою, створення фальшивих новин, що можуть призводити до політичної, соціальної чи економічної дестабілізації.

– кіберзагрози: хакерські атаки на критичну інфраструктуру, державні органи, злам інформаційних систем, крадіжка персональних даних, маніпулювання виборчими процесами.

– психологічний тиск: використання соціальних мереж для формування негативного іміджу уряду, підриву довіри до органів публічного управління.

Ці загрози можуть значно ускладнити управлінські процеси та підвищити рівень ризику для національної безпеки.

Виклики інформаційного забезпечення в умовах гібридних загроз [24].

В умовах гібридних загроз інформаційне забезпечення публічного управління стикається з низкою проблем:

– небезпека дезінформації: у разі поширення недостовірної інформації серед громадян чи посадових осіб, можуть виникнути серйозні політичні чи соціальні кризи. Невірні дані можуть спричиняти паніку, порушення громадського порядку або навіть військові конфлікти.

– зростаюча роль кібербезпеки: державні органи повинні бути готовими до кібератак на критичну інфраструктуру та інформаційні системи, що можуть призвести до порушення нормальної роботи органів публічного управління, крадіжки конфіденційних даних чи маніпуляції виборчими процесами.

– недосконалість законодавства: відсутність чітких норм щодо захисту від інформаційних загроз і кіберзлочинів може ускладнити процес захисту публічного управління від гібридних атак.

– низька готовність до кризових ситуацій: відсутність належної підготовки державних органів та недостатня координація між різними гілками влади можуть значно зменшити ефективність управління в умовах загроз.

Стратегії інформаційного забезпечення в умовах гібридних загроз [28].

Для забезпечення ефективного функціонування публічного управління в умовах гібридних загроз необхідно розробити спеціальні стратегії і заходи, спрямовані на захист та стабільність системи:

1. Створення національних систем захисту інформації: органи влади повинні розробити та запровадити систему захисту від кіберзагроз, включаючи використання сучасних технологій шифрування та безпеки.

2. Посилення інформаційної безпеки: розвиток інструментів моніторингу та протидії дезінформації в медіапросторі, створення централізованих механізмів реагування на кризові ситуації в інформаційному просторі.

3. Навчання та підвищення кваліфікації державних службовців: регулярне навчання працівників органів публічного управління в питаннях кібербезпеки, комунікацій в умовах кризових ситуацій і боротьби з дезінформацією.

4. Міжнародна співпраця: активне залучення до міжнародних ініціатив і організацій для боротьби з транснаціональними інформаційними загрозами, обмін досвідом та ресурсами в сфері інформаційної безпеки.

Інформаційне забезпечення є важливим елементом системи публічного управління, особливо в умовах гібридних загроз [9]. Використання сучасних технологій та засобів комунікації дозволяє підвищити ефективність управлінських процесів, але водночас створює нові виклики у сфері безпеки. Розробка та впровадження відповідних стратегій захисту, модернізація

інформаційних систем та підвищення кваліфікації державних службовців є необхідними кроками для збереження стабільності та ефективності публічного управління в умовах сучасних загроз.

Застосування інформаційних технологій (ІТ) у побудові аналітично-інформаційного забезпечення функціонування публічних органів влади має ключове значення для підвищення ефективності управління, прозорості прийняття рішень, покращення взаємодії з громадянами та забезпечення високого рівня державної служби [44]. Це передбачає використання різноманітних інформаційних систем, аналітичних платформ і інструментів для обробки, аналізу і надання доступу до великих обсягів даних, які стосуються діяльності органів влади.

Інформаційні технології дають змогу автоматизувати численні процеси в публічних органах влади, зокрема:

– електронне урядування (e-Government): Впровадження електронних систем для надання публічних послуг, таких як реєстрація компаній, подача заяв, сплата податків, доступ до публічної інформації тощо.

– електронні документообіг та архіви: Використання електронних платформ для зберігання та обробки документів, що дозволяє скоротити витрати часу та забезпечує зручний доступ до архівних матеріалів.

– системи автоматизованого управління: Вони підтримують роботу органів влади в реальному часі, автоматично збираючи, обробляючи та систематизуючи дані про поточну діяльність.

Аналіз великих даних (Big Data). Використання технологій для збору, зберігання та обробки великих обсягів даних дозволяє органам влади отримувати більш точну картину соціально-економічної ситуації, планувати бюджет, оцінювати ефективність державних програм тощо. Аналітичні інструменти, які працюють з великими даними, дозволяють:

– моніторинг соціальних процесів: Збирати дані з різних джерел (соціальні мережі, публічні звіти, опитування) для аналізу громадської думки.

– прогнозування розвитку регіонів та країн: Використання аналітики для прогнозування економічних і соціальних трендів.

– аналіз ефективності політики: Оцінка впливу різних урядових рішень на соціальну та економічну ситуацію.

Інтелектуальні системи підтримки прийняття рішень (DSS). Інтелектуальні системи підтримки прийняття рішень допомагають керівникам органів влади приймати обґрунтовані, дані рішення на основі аналізу різноманітних інформаційних потоків. Ці системи можуть бути побудовані на таких технологіях, як:

– машинне навчання та штучний інтелект (ШІ): ШІ дозволяє автоматизувати аналіз великих обсягів даних і робити прогнози на основі існуючих тенденцій.

– геоінформаційні системи (ГІС): Допомагають в аналізі територіальних і просторових даних, що дозволяє приймати рішення з урахуванням географічного контексту, наприклад, при плануванні розвитку інфраструктури, управлінні природними ресурсами або виявленні потенційних зон ризику.

Інформаційні платформи для відкритих даних та прозорості. Створення платформ для публікації відкритих даних дає можливість громадянам, бізнесу та аналітичним центрам отримувати доступ до урядової інформації. Це сприяє:

– прозорості та підзвітності: Громадськість може відслідковувати бюджетні витрати, ефективність виконання державних програм, рівень корупції в органах влади.

– активній взаємодії з громадянами: Платформи відкритих даних дозволяють громадянам брати участь у процесі прийняття рішень, подаючи пропозиції або відгуки щодо діяльності уряду.

Системи кібербезпеки та захисту даних.

Зважаючи на високі вимоги до захисту конфіденційних даних, що обробляються публічними органами влади, особливо при використанні

електронних послуг та відкритих платформ, важливим аспектом є впровадження ефективних систем кібербезпеки:

– захист персональних даних: Всі ІТ-системи, що обробляють особисті дані громадян, повинні відповідати вимогам щодо захисту та конфіденційності.

– безпека в електронному урядуванні: Забезпечення захисту від кібератак на державні інформаційні ресурси, захист від несанкціонованого доступу до важливих даних.

Інструменти для участі громадян та цифрова демократія [39]. ІТ-системи забезпечують механізми для більш активної участі громадян у політичних процесах:

– платформи для електронних петицій та голосувань: Дозволяють громадянам виражати свої пропозиції або вимоги до влади, а також брати участь у прийнятті рішень на різних рівнях.

– цифрові консультації та обговорення: Оскільки електронні платформи дозволяють швидко залучати громадськість до обговорень, це допомагає врахувати громадську думку при розробці законодавчих ініціатив або політичних рішень.

Платформи для внутрішньої координації та управління персоналом. Органи влади потребують інструментів для ефективної внутрішньої координації та управління персоналом:

– автоматизовані системи управління персоналом: Для контролю за роботою державних службовців, оцінки їх ефективності та координації діяльності між різними відомствами.

– інструменти для управління проектами: Допомагають в управлінні державними проектами та програмами, зокрема у сфері будівництва, соціальної політики, охорони здоров’я та освіти.

Застосування інформаційних технологій в органах публічної влади дозволяє не лише підвищити ефективність їх роботи, але й покращити якість надання послуг громадянам, збільшити рівень прозорості та підзвітності, а

також залучити громадськість до процесів прийняття рішень. Інтеграція ІТ в управлінські процеси є важливим кроком на шляху до побудови сучасного та ефективного цифрового уряду.

Використання інформаційних технологій в організації інформаційно-аналітичного забезпечення діяльності органів публічного управління є необхідною складовою для підвищення ефективності, прозорості та якості управлінських рішень. У сучасних умовах інформація стала одним із найважливіших ресурсів для прийняття рішень, тому аналітичні системи на базі ІТ стають важливим інструментом для органів публічного управління.

Інформаційно-аналітичне забезпечення (ІАБ) — це система, що включає в себе збирання, обробку, зберігання, аналіз та поширення інформації, яка необхідна для ефективного управління. Системи ІАБ у публічному управлінні мають забезпечувати: відкритість і доступність даних для громадян та відповідних органів. Прозорість процесів ухвалення рішень. Прогнозування та стратегічне планування, яке базується на даних.

Прийняття рішень на основі фактів і даних, а не суб'єктивних припущень.

ІТ-технології дозволяють створити інтегровані платформи для обробки даних з різних джерел, а також інтерактивні інструменти для прийняття рішень.

Основні ІТ-інструменти для інформаційно-аналітичного забезпечення ІТ-технології, що використовуються в ІАБ органів публічного управління, включають в себе такі категорії систем та інструментів:

а) Системи автоматизації документообігу. Для організації роботи з документами та обробки вхідної й вихідної інформації використовуються автоматизовані системи документообігу, які дозволяють:

– забезпечити ефективний контроль за обробкою документів.

– створювати єдині електронні бази даних.

– впроваджувати електронні підписи для забезпечення юридичної сили документів.

б) Геоінформаційні системи (ГІС). ГІС дозволяють аналізувати просторові дані для ухвалення рішень у таких сферах, як:

– управління територіями і ресурсами: Оцінка стану інфраструктури, прогнозування ризиків, управління природними ресурсами.

– картографування і аналіз територій: Визначення зон ризику (наприклад, для боротьби з наслідками стихійних лих).

– управління земельними ресурсами та містобудуванням: Оптимізація розміщення об'єктів, розробка стратегій розвитку.

в) Системи підтримки прийняття рішень (DSS). Ці системи надають адміністраторам та керівникам органів влади необхідні інструменти для аналізу різноманітних даних і прийняття обґрунтованих рішень. До таких систем відносяться:

– інтерфейси для аналізу даних: Інтерфейси, які дозволяють аналізувати статистичні дані, показники економічного розвитку, соціального становища, екологічної ситуації.

– інструменти для моделювання та прогнозування: Допомагають прогнозувати наслідки ухвалених рішень у середньостроковій та довгостроковій перспективі, на основі великих обсягів даних.

г) Системи управління знаннями. Такі системи дозволяють централізовано зберігати й передавати знання та досвід серед державних службовців. Вони допомагають:

– розробляти й підтримувати єдину базу знань, нормативних актів, аналітичних матеріалів.

– систематизувати та оновлювати інформацію для оперативного використання в управлінських рішеннях.

д) Системи моніторингу та оцінки ефективності. Використання IT для моніторингу та оцінки результатів роботи органів влади в реальному часі допомагає:

– виявляти проблемні сфери та своєчасно коригувати стратегії.

– аналізувати виконання планів і програм на всіх рівнях управління.

– забезпечувати публічний доступ до результатів діяльності через відкриті платформи даних.

е) Аналітичні платформи для відкритих даних. Інформаційно-аналітичні платформи, що забезпечують доступ до відкритих даних, сприяють:

– прозорості діяльності державних органів. Громадяни можуть отримувати актуальні дані щодо витрат, виконання програм, корупційних ризиків.

– залученню громадськості до обговорення і оцінки діяльності уряду.

– покращенню зворотного зв'язку між владою і громадянами.

Сучасні технології, що підтримують інформаційно-аналітичне забезпечення. Наразі використовуються передові ІТ-рішення, які дозволяють органам публічного управління ефективно аналізувати дані та приймати рішення:

а) Великі дані (Big Data)

Системи Big Data дозволяють обробляти величезні обсяги інформації з різних джерел, зокрема з соціальних мереж, економічних і політичних індикаторів, що дає змогу:

– аналізувати тренди та поведінкові моделі.

– прогнозувати соціально-економічні процеси.

– оптимізувати державні витрати на основі виведених інсайтів.

б) Машинне навчання та штучний інтелект. Машинне навчання та ШІ забезпечують:

– автоматизацію аналізу даних для виявлення закономірностей та аномалій.

– прогнозування за допомогою алгоритмів на основі історичних даних.

– інтелектуальні системи підтримки прийняття рішень, що дозволяють розглядати різні сценарії розвитку подій.

в) Хмарні технології

Використання хмарних технологій дозволяє:

– зберігати великі обсяги даних і забезпечувати доступ до них з будь-якого місця.

– забезпечувати доступ до інформації у режимі реального часу для всіх учасників управлінського процесу.

– мобільність та гнучкість в роботі органів публічного управління, зокрема для швидкої реакції на кризові ситуації.

Переваги використання ІТ в інформаційно-аналітичному забезпеченні органів публічного управління.

– покращення ефективності прийняття рішень: Використання даних і аналітики дозволяє приймати більш обґрунтовані рішення, зменшуючи суб'єктивність і помилки.

– прозорість і підзвітність: Відкритість даних і аналітичних результатів для громадян і організацій забезпечує більшу прозорість діяльності органів влади.

– зниження витрат: Автоматизація та оптимізація процесів дозволяють скоротити час і ресурси на виконання управлінських завдань.

– покращення взаємодії з громадянами: Залучення громадськості до процесів прийняття рішень і зворотного зв'язку допомагає підвищити довіру до державних органів.

Інформаційно-аналітичне забезпечення є критично важливим елементом у діяльності органів публічного управління, оскільки воно забезпечує основу для прийняття ефективних управлінських рішень, формує прозорість і підзвітність, а також сприяє розвитку демократичних процесів у країні [53]. Використання сучасних ІТ-інструментів дозволяє оптимізувати внутрішні процеси, здійснювати моніторинг і оцінку ефективності державної

політики, а також забезпечувати активну взаємодію з громадянами через відкриті платформи даних і цифрові інструменти.

2.2 Аналіз процесу формування інформаційного забезпечення публічного управління в умовах гібридних загроз

Аналіз процесу формування інформаційного забезпечення публічного управління в умовах гібридних загроз вимагає врахування ряду аспектів, пов'язаних з використанням інформаційних технологій, організацією комунікаційних процесів, захистом від кіберзагроз і управлінням кризовими ситуаціями, що виникають через неочікувані та часто складні загрози [5].

Інформаційне забезпечення публічного управління — це сукупність даних, знань, інформаційних систем і технологій, які використовуються органами публічної влади для виконання їхніх функцій і забезпечення ефективного управління. Умови гібридних загроз вимагають специфічних підходів до організації цього процесу, оскільки сучасні виклики полягають не лише у традиційних формах атак, а й у комбінованих стратегіях, що використовують як інформаційні, так і неінформаційні методи впливу [29].

Гібридні загрози є комбінацією традиційних (військових) і нетрадиційних (інформаційних, економічних, політичних) засобів впливу, спрямованих на підрив стабільності держави або суспільства. Вони характеризуються використанням інформаційних технологій для маніпулювання громадською думкою, поширення дезінформації, кібернападів, а також економічних санкцій і дипломатичних заходів.

В контексті публічного управління важливо:

– оцінити загрози в інформаційному середовищі: Оскільки гібридні загрози можуть включати інформаційні операції, атаки на критичну інфраструктуру або використання медіа та соціальних мереж для маніпулювання населенням, публічні органи повинні мати систему моніторингу та аналітики, здатну виявляти такі загрози.

– розробити антикризові заходи: Важливо мати механізми швидкого реагування на кризові ситуації, які включають як стратегії кібербезпеки, так і методи контрпропаганди.

– враховувати інтеграцію технологій і методів: Для управління інформацією в умовах гібридних загроз необхідне використання передових інформаційних технологій, зокрема штучного інтелекту, для моніторингу та аналізу великих обсягів даних, а також систем захисту від кіберзагроз.

Основні складові інформаційного забезпечення публічного управління в умовах гібридних загроз:

1. Інформаційні системи та платформи: Розробка та впровадження спеціалізованих систем для обробки та зберігання інформації, яка стосується безпеки держави, забезпечення оперативного обміну інформацією між державними органами, а також із громадськістю. Такі системи мають бути стійкими до кібернападів та маніпуляцій.

2. Аналіз та оцінка загроз: Створення аналітичних центрів, які займаються дослідженням потенційних загроз і формують стратегії захисту від них. Вони використовують методи прогнозування та оцінки ризиків на основі великих даних і машинного навчання.

3. Інформаційна безпека: Одним із ключових аспектів є захист інформаційних систем від кіберзагроз, таких як хакерські атаки, витоки даних та інші форми злому. Для цього потрібні сучасні технології захисту інформації, а також навчання і підготовка персоналу для роботи в умовах кіберзагроз.

4. Стратегії комунікації з громадськістю: В умовах гібридних загроз важливо мати ефективні канали комунікації, що дозволяють владі швидко реагувати на спотворену інформацію або дезінформацію, що поширюється через соціальні мережі. Це може включати в себе як використання офіційних каналів (новини, державні соцмережі), так і співпрацю з незалежними ЗМІ.

5. Розвиток кадрового потенціалу: Публічне управління в умовах гібридних загроз потребує висококваліфікованих фахівців у галузі

інформаційних технологій, аналітики, кібербезпеки, а також менеджерів, здатних адаптувати організацію до нових викликів. Постійне навчання та тренування кадрів, проведення симуляцій кризових ситуацій є важливою частиною стратегії.

Виклики та рекомендації:

– технічні виклики: Необхідність постійного оновлення і модернізації технологічної інфраструктури для забезпечення стійкості до нових типів кіберзагроз.

– правові та етичні питання: Створення нормативно-правових актів для регулювання діяльності в сфері кібербезпеки, захисту даних та інформаційної безпеки. Це включає баланс між забезпеченням безпеки та правами громадян.

– координація між державними і приватними структурами: Важливою складовою є налагодження ефективної співпраці між державними органами та приватними компаніями, які відповідають за кібербезпеку, комунікації і надають технологічні рішення.

Формування інформаційного забезпечення публічного управління в умовах гібридних загроз є складним, але важливим процесом для забезпечення національної безпеки та стабільності держави [44]. Окрім використання сучасних інформаційних технологій і методів захисту, важливою є здатність органів публічного управління швидко адаптуватися до змінюваного середовища, яке характеризується новими типами загроз. У цьому контексті особлива увага має приділятися розвитку аналітичних центрів, комунікаційних стратегій та систем захисту інформаційних ресурсів держави.

Додамо, що зауваження про роль маркетингу як джерела знань та світового досвіду успішної ринкової діяльності в контексті розв’язання проблем інформаційного забезпечення публічного управління в умовах гібридних загроз є дуже цікавим і важливим. Дійсно, маркетинг може стати потужним інструментом у цьому процесі, оскільки він сприяє створенню

стратегії, яка об’єднує управління інформацією, ефективні комунікації та мобілізацію ресурсів для швидкого реагування на нові загрози.

Маркетинг в контексті публічного управління — це не лише про рекламу чи просування товарів і послуг, а й про створення ефективних каналів комунікації між урядовими органами, громадськістю та іншими зацікавленими сторонами [11]. Творче застосування маркетингових принципів може допомогти у:

– виявленні потреб і запитів громадян: Як у бізнесі, так і в публічному управлінні важливо розуміти потреби аудиторії (у даному випадку громадян). Використовуючи маркетингові дослідження, органи влади можуть отримувати зворотний зв'язок, аналізувати настрої громадян і виявляти можливі ризики, які можуть виникнути через неправильно сприйняту інформацію або дезінформацію.

– керуванні репутацією: У кризових ситуаціях, коли гібридні загрози можуть впливати на довіру до державних інститутів, маркетинг допомагає формувати стратегії для відновлення і зміцнення репутації через прозорість, відповідальність та ефективну комунікацію.

– управлінні брендом держави: Сучасний маркетинг активно використовує концепцію «бренду», і в цьому контексті держави. Розвиток позитивного іміджу держави на міжнародній арені, особливо в умовах гібридних загроз, допомагає зберегти стабільність і сприяє залученню інвестицій, міжнародної підтримки та розвитку зовнішньоекономічних зв’язків.

Для того щоб інформаційне забезпечення публічного управління було ефективним в умовах гібридних загроз, необхідно застосовувати комплексні маркетингові стратегії:

– комунікація через нові канали: Соціальні мережі, мобільні додатки та цифрові платформи дозволяють державі безпосередньо взаємодіяти з громадянами, коригуючи курс і транслюючи важливу

інформацію. Використання маркетингових інструментів для популяризації офіційних каналів комунікації є важливим для боротьби з дезінформацією.

– позиціонування державних ініціатив: Як і в ринковій діяльності, для успішного просування державних ініціатив необхідно використовувати стратегії позиціонування. Це означає, що кожна ініціатива, будь то боротьба з кіберзагрозами чи антикризові програми, повинна мати чітке і привабливе представлення, що підвищує її сприйняття серед населення.

– аналіз конкурентів: Маркетингові дослідження часто включають аналіз конкурентів. У публічному управлінні це може бути метафорою для аналізу держав, які використовують подібні стратегії в умовах гібридних загроз. Вивчення досвіду інших країн дає можливість розробляти власні стратегії і уникати можливих помилок.

Маркетинг у сучасному світі не обходиться без аналітики даних, і публічне управління може скористатися цими підходами для забезпечення ефективного реагування на загрози:

– Big Data та аналіз громадської думки: Використання великих даних для аналізу поведінки населення та виявлення потенційних кризових ситуацій може допомогти швидко реагувати на загрози. Інструменти аналізу настроїв в Інтернеті, соціальних мережах і новинних платформах можуть допомогти державним органам зрозуміти, як інформація сприймається громадянами і як з нею можна працювати.

– маркетингова автоматизація: В умовах гібридних загроз швидкість реакції є ключовою. Технології автоматизації маркетингових процесів, які дозволяють швидко поширювати інформацію, запускати інформаційні кампанії або давати відповіді на запити громадян через чат-ботів, можуть стати важливим елементом стратегії публічного управління.

Маркетинг, як джерело знань та досвіду, орієнтується на інноваційність і швидку адаптацію до змінюваних умов ринку [51]. Публічне управління може впроваджувати інноваційні стратегії, щоб забезпечити:

– гнучкість і швидкість реагування: У разі виникнення нових загроз або кризових ситуацій, необхідно швидко перебудовувати стратегії, використовувати нові канали комунікації та ефективно мобілізувати ресурси. Інноваційний підхід до маркетингових стратегій може бути орієнтований на використання новітніх технологій для моніторингу та управління інформаційними потоками.

– креативні методи боротьби з дезінформацією: Творче застосування маркетингових стратегій дозволяє створювати контркампанії, що сприяють правильному інформуванню громадськості та запобігають впливу фальшивих новин або маніпуляцій.

У сучасному світі маркетинг може стати важливим елементом в управлінні інформацією та подоланні викликів гібридних загроз, що виникають перед публічним управлінням [6]. Креативний підхід, орієнтований на ефективну комунікацію, використання нових технологій і інноваційних стратегій, може допомогти органам публічної влади не лише успішно протистояти інформаційним загрозам, але й підвищити рівень довіри до державних інститутів.

На нашу думку, вирішення таких проблем залежить від того, наскільки творчо і цілеспрямовано використовується маркетинг як джерело знань і світового досвіду успішної ринкової діяльності. На рисунку 2.1 наведені найвідоміші визначення маркетингу, яких сьогодні налічується більше двох тисяч.

Аналіз зарубіжного досвіду маркетингу в публічному управлінні дає змогу виявити ефективні стратегії, які сприяють поліпшенню взаємодії між органами влади та громадянами, а також підвищенню прозорості та якості надання публічних послуг. Застосування маркетингових принципів у державному секторі здобуло популярність завдяки своєму потенціалу у вирішенні проблем, таких як низька довіра громадян до влади, незадоволеність якістю послуг та необхідність модернізації адміністративних процесів.

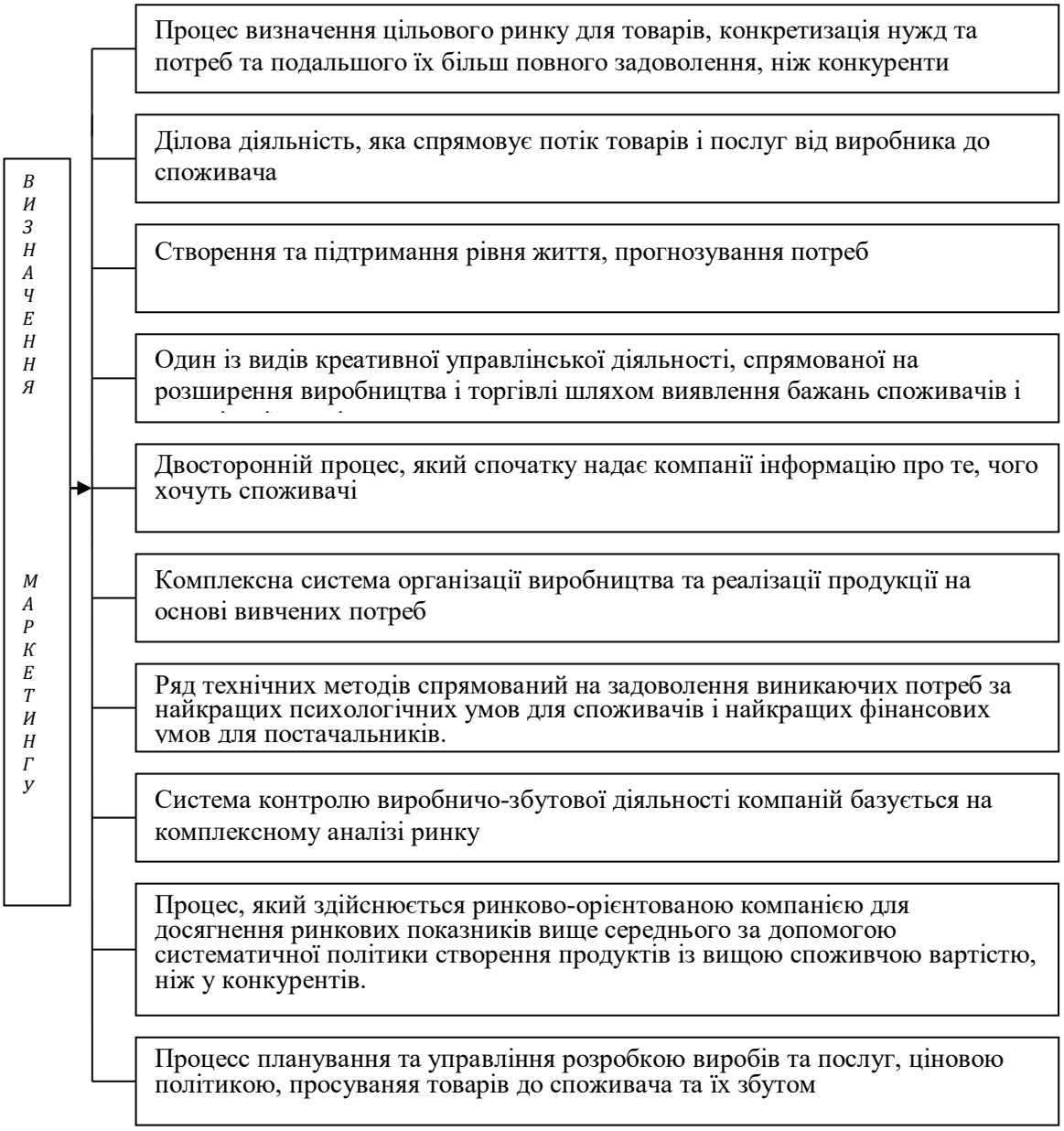

Рисунок 2.1 - Дефініція процесу маркетингу у літературі

Ось деякі ключові аспекти зарубіжного досвіду маркетингу в публічному управлінні:

1. Залучення громадян через комунікацію та участь. У багатьох країнах маркетинг публічних послуг включає в себе активну комунікацію з громадянами. Влада використовує різноманітні комунікаційні канали (вебсайти, соціальні мережі, мобільні додатки) для того, щоб забезпечити зворотний зв'язок з громадянами. Ось кілька прикладів:

– Австралія: В Австралії використовуються онлайн-платформи, які дозволяють громадянам брати участь в урядових ініціативах через опитування, обговорення та голосування. Це допомагає органам влади краще розуміти потреби населення і ефективно адаптувати свої політики.

– Скандинавські країни (Швеція, Данія, Фінляндія): Активне використання цифрових технологій для підвищення ефективності адміністративних процесів, таких як електронні послуги для громадян і інтерактивні платформи для збору думок та пропозицій.

2. Стратегічний маркетинг для покращення публічних послуг. Маркетингові стратегії в державному секторі орієнтовані на підвищення якості та доступності публічних послуг. Це включає:

– Фінляндія: Країна активно використовує маркетингові стратегії для покращення іміджу урядових програм, зокрема в галузі охорони здоров'я та освіти. Використання сучасних інформаційних технологій, персоналізованих послуг, зручних інтерфейсів для доступу до держпослуг є ключовими факторами успіху.

– Нідерланди: У Нідерландах державні органи використовують принципи маркетингу для оптимізації процесів надання послуг через цифрові канали, включаючи мобільні додатки для взаємодії з державними установами.

3. Імідж державних установ та брендинг

Маркетинг у публічному управлінні також включає розвиток іміджу органів влади як брендів, що мають чітке, зрозуміле та позитивне сприйняття серед громадян. Це важливо для створення довіри до інститутів влади та для покращення громадянської активності.

– Сінгапур: Уряд Сінгапуру активно використовує брендинг та стратегічний маркетинг для формування позитивного іміджу державних ініціатив, таких як кампанії з охорони навколишнього середовища, розвитку інноваційних технологій і підтримки громадянської участі.

– Великобританія: Кампанії для підвищення обізнаності громадян щодо послуг уряду, таких як реєстрація на вибори або програми підтримки безробітних, часто використовують маркетингові принципи для зміцнення зв'язку між громадянами та урядом.

4. Сегментація та персоналізація послуг

Державні установи в багатьох країнах застосовують маркетингові техніки сегментації та персоналізації, щоб краще задовольняти різні потреби громадян:

– Канада: Канадський уряд застосовує сегментацію для надання державних послуг, орієнтуючись на різні соціальні групи, такі як пенсіонери, молодь, підприємці, що дозволяє максимально ефективно адаптувати програми до їхніх потреб.

– Німеччина: Сегментація громадян за інтересами та соціальним статусом для надання різних видів підтримки або послуг, зокрема для вразливих груп населення, таких як іммігранти або малозабезпечені верстви.

5. Антикризові комунікації

Маркетинг в публічному управлінні також включає ефективну кризову комунікацію, що дозволяє зберігати довіру до органів влади під час надзвичайних ситуацій або криз.

– США: В умовах пандемії COVID-19 уряди штату та федеральні органи США використовували маркетингові стратегії для просування кампаній щодо вакцинації та підтримки економічної стабільності. Інтерактивні цифрові платформи, спільні рекламні кампанії і масова інформація допомогли мобілізувати громадян.

– Японія: Японія активно використовувала маркетингові стратегії для інформування громадян під час стихійних лих, таких як землетруси чи цунамі, через мобільні додатки, спеціалізовані телеканали та інші канали комунікації.

6. Цифрові інструменти та електронне урядування. Використання цифрових технологій в публічному управлінні дозволяє значно покращити

ефективність надання послуг, зокрема через платформи електронного урядування.

– Естонія: Естонія є одним з лідерів у галузі електронного урядування, де громадяни можуть отримувати майже всі державні послуги онлайн. Естонія застосовує маркетингові підходи для популяризації електронних послуг та стимулювання користування ними.

– Південна Корея: Країна активно інтегрує цифрові інструменти для надання послуг і забезпечення доступу до державних баз даних через онлайн-платформи та мобільні додатки.

Зарубіжний досвід маркетингу в публічному управлінні демонструє значний потенціал для підвищення ефективності роботи державних установ, покращення взаємодії з громадянами, підвищення прозорості та доступності послуг. Стратегії залучення громадян, покращення іміджу урядових інституцій та використання цифрових інструментів є ключовими елементами, які можуть бути адаптовані до умов українського публічного управління для досягнення більш ефективних результатів.

2.3 Аналіз сучасного стану впровадження інформаційного забезпечення інформаційних технологій у системі публічного управління міста Харкова в умовах гібридних загроз

Аналіз сучасного стану впровадження інформаційного забезпечення інформаційних технологій у системі публічного управління міста Харкова передбачає оцінку використання інформаційних технологій (ІТ) для оптимізації управлінських процесів, покращення комунікації з громадянами та підвищення ефективності функціонування органів місцевої влади.

Харків є одним з провідних міст України у сфері інформаційних технологій [30]. Місто активно розвивається в напрямку цифровізації публічного управління, що є важливим елементом стратегії розвитку. Харків є важливим технологічним центром з потужною ІТ-екосистемою, що

включає не лише комерційні IT-компанії, але й високий рівень освіти в галузі технологій. В умовах глобалізації та цифровізації суспільства влада Харкова активно інтегрує новітні технології у свою діяльність, що сприяє вдосконаленню адміністративних процесів і взаємодії з громадянами [32].

Основні напрямки впровадження IT у публічне управління:

1. Електронні послуги для громадян

Одним із ключових напрямків є розширення та удосконалення електронних послуг для мешканців міста. Вже кілька років поспіль у Харкові працюють платформи, які дозволяють жителям подати заяви на отримання різноманітних послуг через інтернет, не відвідуючи державні установи:

– портал міських послуг — на цьому порталі харків'яни можуть подавати заявки на отримання адміністративних послуг, таких як реєстрація майна, оформлення дозвільних документів тощо.

– мобільні додатки — для покращення доступу до послуг та інформації запущені мобільні додатки, які дозволяють отримувати актуальні новини міста, подавати звернення до органів влади, а також отримувати сповіщення про стан справ.

Інформаційні технології активно використовуються для управління міською інфраструктурою. Вони допомагають оптимізувати процеси в таких сферах, як:

– транспорт: Впровадження інтелектуальних транспортних систем (ITS), що включають моніторинг дорожнього руху, інформаційні табло та системи для управління міським транспортом.

– енергетика: Впровадження «розумних» лічильників для моніторингу споживання енергії та води, а також систем для ефективного управління енергетичними ресурсами.

– міська інфраструктура: Системи для управління водопостачанням, водовідведенням, освітленням, а також аналіз даних для виявлення проблемних ділянок у міській інфраструктурі.

Використання ІТ в управлінських процесах міста Харкова включає автоматизацію внутрішніх адміністративних процедур:

– електронний документообіг — значне скорочення паперових документів і спрощення процедур завдяки автоматизації документообігу.

– CRM-системи для зворотного зв’язку з громадянами — надання можливості мешканцям міста залишати запити, звернення, скарги через онлайн-системи, що дозволяє оперативно реагувати на проблеми.

З метою забезпечення прозорості діяльності місцевої влади в місті впроваджуються платформи для відкритих даних [56]. Це дозволяє громадянам і бізнесу отримувати доступ до інформації про діяльність міських органів, бюджет, державні закупівлі, екологічні дані та інші важливі аспекти.

Проблеми та виклики впровадження ІТ у публічному управлінні:

Інфраструктурні та фінансові обмеження. Попри високий потенціал, впровадження новітніх ІТ-рішень у публічному управлінні стикається з низкою труднощів [42]. Однією з основних проблем є обмежене фінансування для масштабних проектів, особливо у контексті важливих інфраструктурних змін, таких як оновлення мереж і програмного забезпечення.

Кібербезпека. З ростом цифрових послуг зростають й ризики кібератак, що ставить під загрозу конфіденційність даних та безпеку користувачів. Впровадження ефективних заходів з кібербезпеки є необхідною умовою для розвитку цифрової адміністрації.

Підвищення кваліфікації персоналу. Для успішної реалізації проектів з цифровізації потрібні кваліфіковані кадри, які здатні працювати з сучасними ІТ-системами. Влада має розвивати програми підвищення кваліфікації для своїх працівників.

Перспективи розвитку ІТ у публічному управлінні Харкова.

У найближчій перспективі важливим напрямком розвитку є:

– розширення системи "розумного міста" (Smart City) — розвиток інфраструктури для моніторингу та управління міськими процесами в реальному часі, таких як транспорт, енергозабезпечення та комунальні послуги.

– покращення взаємодії з громадянами — інтеграція новітніх технологій для забезпечення зручного та швидкого зворотного зв’язку між органами влади та громадянами.

– інноваційні ІТ-рішення для сталого розвитку — використання інформаційних технологій для вирішення проблем сталого розвитку, таких як управління природними ресурсами та мінімізація екологічного сліду.

Аналіз сучасного стану впровадження інформаційного забезпечення в системі публічного управління міста Харкова в умовах гібридних загроз є важливим етапом для розуміння того, як технології та інфраструктура можуть посилити ефективність управлінських процесів, а також забезпечити стійкість до різноманітних загроз [46]. Зважаючи на те, що Харків є одним з найбільших і найважливіших міст України, це питання має стратегічне значення для розвитку місцевого самоврядування, а також національної безпеки.

На сьогоднішній день місто Харків активно працює над модернізацією своєї інформаційної інфраструктури в рамках розвитку розумних міст (smart cities). Це включає в себе:

– електронне урядування: розвиток онлайн-платформ для надання адміністративних послуг громадянам, таких як портал "Громадський бюджет", електронний реєстр для організацій міського самоврядування, цифрові реєстри для моніторингу соціальних послуг, земельних та будівельних питань.

– інтеграція з національними системами: Харків активно взаємодіє з державними інформаційними системами, такими як система електронного голосування, реєстрація юридичних осіб, реєстри з охорони здоров'я та освіти.

– системи моніторингу та управління інфраструктурою: використання "розумних" технологій для управління дорожнім рухом, моніторинг рівня забруднення повітря, управління водо- та енергозабезпеченням, а також для забезпечення безпеки через системи відеоспостереження.

Гібридні загрози, що мають місце в умовах сучасної геополітичної ситуації, суттєво змінюють підходи до організації інформаційної безпеки. До таких загроз відносяться:

– кіберзагрози та кібернапади: включають спроби кібератак на критичну інфраструктуру міста, зокрема на системи управління міськими ресурсами, бази даних громадян, системи комунікацій та управління транспортом. Гібридні атаки можуть сприяти паралізації роботи органів влади або розповсюдженню дезінформації.

– дезінформаційні кампанії: маніпуляції з інформацією можуть підривати довіру до місцевої влади та створювати соціальну напругу. Враховуючи важливість інформаційних ресурсів для управління містом, такі кампанії можуть негативно вплинути на ефективність публічного управління.

– глобальні та локальні інформаційні війни: політичні ідеології, які поширюються через цифрові платформи, можуть мати вплив на громадську думку, інформувати або дезінформувати про хід політичних чи соціальних процесів.

У відповідь на ці виклики міська влада Харкова активно розвиває кілька напрямів для посилення кіберстійкості та безпеки інформаційних систем:

– кіберзахист: створення та модернізація системи кібербезпеки, включаючи розгортання мережевих фільтрів, систему виявлення вторгнень, регулярні тренування для персоналу з реагування на кіберінциденти, впровадження засобів криптографічного захисту інформації.

– захист інфраструктури: важливими є заходи з фізичного захисту критичних об'єктів інфраструктури та резервного копіювання даних.

– цифрові платформи для взаємодії з громадянами: розвиток платформ для публічного обговорення важливих рішень, забезпечення прозорості та залучення громади до управлінських процесів через мобільні додатки та онлайн-послуги.

На майбутнє міська влада Харкова має кілька стратегічних цілей:

– посилення кіберстійкості: створення на базі муніципалітету спеціальних центрів реагування на кіберзагрози, підвищення рівня підготовки та свідомості серед працівників органів публічного управління.

– розвиток “розумного” міста: інтеграція нових інформаційних технологій в усі сфери міського життя, використання Інтернету речей (IoT) для оптимізації міських процесів (збирання сміття, управління трафіком, енергозбереження).

– партнерство з приватним сектором та міжнародними організаціями: залучення технологічних компаній та міжнародних партнерів до співпраці в питаннях кібербезпеки та цифровізації адміністративних процесів.

Загалом, Харків робить суттєвий крок уперед у напрямку цифровізації публічного управління. Використання сучасних інформаційних технологій допомагає покращити ефективність адміністративних процесів, підвищити прозорість управління та забезпечити зручні умови для мешканців. Однак для успішної реалізації цих ініціатив важливими є інвестиції в інфраструктуру, кібербезпеку та підвищення кваліфікації кадрів.

Упровадження інформаційних технологій у систему публічного управління міста Харкова є важливим кроком до забезпечення ефективного, прозорого та стійкого управління, однак в умовах гібридних загроз важливо приділяти особливу увагу питанням кібербезпеки та інформаційної стійкості. Відповідні заходи з захисту від кіберзагроз і дезінформації, а також посилення цифрової інфраструктури можуть забезпечити не лише безпеку управлінських процесів, а й сприяти розвитку міста в умовах постійної змінної загрози.

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

3.1 Впровадження сучасних інформаційних технологій у систему публічного управління

Удосконалення інформаційного забезпечення системи публічного управління в умовах гібридних загроз є актуальним завданням для державних органів, оскільки зростаюча складність і різноманіття цих загроз вимагають ефективних методів для забезпечення стабільності та безпеки країни [38]. Гібридні загрози поєднують в собі різні форми і методи впливу: від інформаційних війн і кібератак до маніпуляцій суспільною свідомістю та економічного саботажу.

Ось основні напрямки удосконалення інформаційного забезпечення публічного управління в таких умовах:

1. Розвиток інфраструктури кібербезпеки

– інвестиції в інфраструктуру кібербезпеки: Створення потужних і надійних захисних систем, здатних протистояти кібератакам, фішингу, DDoS-атакам та іншим видам кіберзагроз.

– моніторинг та аналітика кіберзагроз: Встановлення систем моніторингу для оперативного виявлення та аналізу кіберзагроз, забезпечення безпеки комунікацій та даних.

– підвищення кваліфікації фахівців: Підготовка кадрів, здатних ефективно реагувати на кіберзагрози, та впровадження механізмів швидкої адаптації до нових технологій і загроз.

2. Системи протидії дезінформації та маніпуляціям

– моніторинг інформаційного простору: Виявлення фейкових новин, маніпуляцій та пропаганди через соціальні мережі, медіа-ресурси, сайти та інші канали.

– покращення медіаграмотності громадян: Навчання населення критичному мисленню і перевірці інформації, що поширюється через різні канали.

– забезпечення прозорості публічної інформації: Створення відкритих платформ для доступу до державних даних і інформації, що дозволяє знизити вплив маніпуляцій на громадську думку.

3. Автоматизація та цифровізація публічного управління

– розвиток е-урядування: Впровадження та вдосконалення електронних систем управління, що забезпечують зручний та швидкий доступ до публічних послуг для громадян і бізнесу.

– цифрові платформи для взаємодії з громадянами: Створення інтегрованих платформ для збору та обробки даних про потреби населення, надання онлайн-консультацій та зворотного зв'язку.

– інтеграція великих даних (Big Data) і штучного інтелекту (AI): Використання аналізу великих даних для виявлення тенденцій і проблемних ситуацій, що дозволяє оперативно реагувати на потенційні загрози.

4. Забезпечення гнучкості та швидкості прийняття рішень

– системи кризового управління: Створення центрів кризового реагування та ситуаційних центрів, що дозволяють швидко реагувати на різні гібридні загрози.

– моделювання сценаріїв загроз: Впровадження технологій прогнозування та сценарного аналізу для підготовки до можливих загроз та гнучкого реагування на них.

– тренування та симуляції для державних органів: Регулярні навчання та симуляції для органів державної влади, що дозволяють підвищити їх ефективність у разі виникнення надзвичайних ситуацій.

5. Міжнародне співробітництво та координація

– обмін інформацією з іншими державами: Розширення міжнародного співробітництва у сфері кібербезпеки та боротьби з дезінформацією.

– підтримка міжнародних стандартів і протоколів безпеки: Адаптація національних стандартів до міжнародних норм та вимог щодо захисту інформації, кібербезпеки та боротьби з гібридними загрозами.

– спільні навчання та координація: Спільні навчання з міжнародними партнерами для відпрацювання спільних відповідей на гібридні загрози.

6. Розвиток правових і нормативних основ

– оновлення законодавства: Прийняття та удосконалення законодавства, що стосується кібербезпеки, захисту даних, боротьби з пропагандою та маніпуляціями в медіа.

– створення інституцій для протидії загрозам: Створення спеціалізованих органів для боротьби з дезінформацією, кіберзлочинністю та іншими гібридними загрозами.

– механізми правового реагування на загрози: Розробка механізмів для правового реагування на нові форми загроз, зокрема через санкції, позови до суду та міжнародну співпрацю.

7. Забезпечення прозорості та підзвітності

– залучення громадян до управління: Використання громадянських платформ для участі в управлінських процесах, зокрема через електронні петиції, опитування та зворотний зв'язок.

– моніторинг діяльності органів влади: Впровадження систем незалежного моніторингу та аудитів для оцінки ефективності публічного управління та запобігання корупції.

– підвищення відкритості інформації: Політика відкритих даних, щоб громадяни могли отримувати доступ до інформації про діяльність держави.

8. Розвиток національної стійкості та соціальної згуртованості

– підвищення довіри громадян до органів влади: Робота з громадянами для підвищення їхнього довіри до інституцій та розуміння важливості боротьби з гібридними загрозами.

– психологічна стійкість і підтримка: Проведення кампаній для покращення психологічної стійкості громадян, підтримки національної єдності, зменшення соціальних напружень.

Гібридні загрози є багатоаспектними та складними, тому удосконалення інформаційного забезпечення публічного управління повинно базуватися на інтеграції новітніх технологій, розвитку міжнародної співпраці, зміцненні кібербезпеки, а також постійному вдосконаленні правових і управлінських практик [43]. Це дозволить державі ефективно протистояти сучасним загрозам і забезпечити стабільність та безпеку для громадян.

Впровадження сучасних інформаційних технологій (ІТ) у систему публічного управління є важливим кроком на шляху до покращення ефективності, прозорості та доступності державних послуг. Це дозволяє підвищити якість управлінських рішень, зменшити корупцію, оптимізувати витрати і збільшити довіру громадян до державних інститутів. Розробка умов для впровадження ІТ в публічному управлінні потребує системного підходу, включаючи технічні, організаційні та правові аспекти.

1. Інфраструктура та технічні умови

– розвиток цифрової інфраструктури: Забезпечення доступу до швидкісного інтернету, створення центрів обробки даних (ЦОД) та інших технологічних хабів.

– модернізація технічного обладнання: Оснащення державних установ сучасними комп’ютерними системами, серверним обладнанням, а також забезпечення безпеки інформаційних систем.

– інтеграція інформаційних систем: Розробка та впровадження інтегрованих платформ для обміну даними між різними державними органами та рівнями влади.

– інтероперабельність: Забезпечення сумісності між різними ІТ-системами, що дозволяє автоматично обмінюватися даними між органами влади, без дублювання і зниження ймовірності помилок.

2. Організаційні умови

– створення відповідних структур: Формування окремих органів або підрозділів для управління ІТ-процесами в державних установах, таких як департаменти цифрових технологій або державні агентства, відповідальні за цифрові трансформації.

– навчання та кваліфікація кадрів: Підготовка та перепідготовка держслужбовців в галузі ІТ-навичок, електронного урядування, захисту даних та роботи з новими технологіями.

– процеси управління змінами: Розробка та впровадження механізмів управління змінами в організаціях, що включають планування, моніторинг та адаптацію нових технологій до існуючих процесів управління.

3. Правові умови

– розробка законодавчої бази: Оновлення та прийняття нових нормативно-правових актів, що регулюють використання інформаційних технологій у публічному управлінні. Це включає питання електронного урядування, захисту персональних даних, інтелектуальної власності та кібербезпеки.

– права та обов'язки громадян і органів влади: Чітке визначення прав і обов'язків громадян щодо використання електронних послуг, а також відповідальності державних органів за надання цих послуг.

– захист даних та кібербезпека: Розробка заходів для забезпечення кібербезпеки, захисту інформації та боротьби з кіберзагрозами. Включає створення національних стандартів безпеки даних, захисту від несанкціонованого доступу до державних інформаційних систем.

4. Фінансові умови

– фінансування та інвестиції: Залучення державних та приватних інвестицій для фінансування цифрових трансформацій. Використання

міжнародних грантів, фінансових програм і співпраці з міжнародними організаціями.

– ефективне управління ресурсами: Оцінка витрат на цифрову трансформацію та забезпечення довгострокового фінансування підтримки та оновлення IT-інфраструктури.

5. Інноваційні технології

– використання новітніх технологій**: Впровадження таких інновацій, як штучний інтелект, великі дані (Big Data), блокчейн, Інтернет речей (IoT) в управлінські процеси для покращення ефективності та прозорості.

– електронне урядування (e-Government): Створення єдиного порталу для надання державних послуг онлайн, спрощення бюрократичних процедур через автоматизацію.

6. Соціальні умови

– цифрове включення громадян: Розвиток програм для покращення цифрових навичок населення, щоб забезпечити доступність електронних послуг для всіх верств населення, включаючи пенсіонерів, осіб з обмеженими можливостями та інших соціально вразливих груп.

– інформування та взаємодія з громадянами: Створення каналів комунікації для швидкого інформування громадян про нові послуги та можливості, а також збору зворотного зв’язку щодо якості надання публічних послуг.

7. Моніторинг та оцінка

– система моніторингу і оцінки ефективності: Розробка та впровадження механізмів для постійного моніторингу впровадження IT-рішень в публічному управлінні, включаючи вимірювання ефективності, виявлення недоліків та вчасне їх коригування.

– звітування та прозорість: Забезпечення регулярного звітування про результати цифрових ініціатив, їх вплив на покращення управління та надання послуг.

8. Залучення громадян і партнерів

– співпраця з приватним сектором: Створення партнерств між державними органами та приватними компаніями, що мають досвід у розробці ІТ-рішень, для забезпечення найкращих практик та інновацій.

– взаємодія з міжнародними організаціями: Співпраця з міжнародними організаціями для отримання експертної підтримки, навчання, а також для залучення міжнародних фінансових ресурсів.

Для ефективного впровадження сучасних ІТ у публічне управління необхідно не лише технічне оснащення, а й комплексний підхід, що включає організаційні, правові, фінансові та соціальні умови. Потрібно створити ефективну цифрову інфраструктуру, забезпечити захист даних, навчати кадри та мотивувати громадян до участі в цифрових процесах. Всі ці елементи разом допоможуть забезпечити успішну цифрову трансформацію публічного управління та покращити якість життя громадян [62].

Діяльність зі створення Мережі за останні чотири десятиліття можна умовно поділити на чотири основні етапи:

1. Початковий етап (1970-1980-ті роки) — Розвиток основ інфраструктури:

– основні події: У 1970-х роках відбулося формування базових технологій для створення глобальних мереж. Один із найважливіших етапів — створення ARPANET (середина 1960-х), яка стала основою для майбутнього Інтернету.

– технології**: Основи пакетної комутації, перші протоколи передачі даних (наприклад, TCP/IP), а також створення перших комунікаційних стандартів для мереж.

2. Етап комерціалізації та розширення (1990-ті роки) — Масове поширення Інтернету

– основні події: У 1990-х роках Інтернет почав виходити за межі військових і наукових установ і став доступним для широкого кола

користувачів. Введення World Wide Web (WWW) на чолі з Тімом Бернерсом-Лі в 1991 році значно спростило використання Інтернету.

– технології: Впровадження браузерів, розвиток HTML, HTTP та інших веб-технологій. Початок ери комерційних послуг в Інтернеті, поштових систем, пошукових систем і перших вебсайтів.

– соціальні зміни: Створення перших великих веб-компаній, таких як Amazon, Yahoo, Google, а також популяризація Інтернету серед широкої аудиторії.

3. Етап інтеграції та діджиталізації (2000-2010-ті роки) — Інтернет стає частиною повсякденного життя:

– основні події: Інтернет став повноцінною частиною повсякденного життя. Розвиток широкосмугового Інтернету, мобільних технологій, соціальних мереж і відео- та медіасервісів.

– технології: Масове впровадження Wi-Fi, 3G, 4G, а також розвиток смартфонів та планшетів. Поширення хмарних технологій, електронної комерції, відео-стримінгових сервісів (наприклад, YouTube, Netflix).

– соціальні зміни: Зростання соціальних медіа, таких як Facebook, Twitter, Instagram, а також зміни в способах взаємодії людей через Інтернет — віртуальні громади, онлайн-ігри, блоги.

4. Етап нових технологій та інновацій (2010-2020-ті роки і до сьогодні) — Інтернет як інфраструктура для розвитку нових технологій:

– основні події: Інтернет став не лише платформою для взаємодії людей, але й основою для розвитку нових технологій: Інтернет речей (IoT), штучний інтелект, блокчейн, 5G, великі дані (Big Data).

– технології: Інтернет речей (IoT), блокчейн, AI, автоматизація, бездротові мережі 5G, автономні системи. Розвиток великих інтернет-компаній, таких як Google, Amazon, Apple, Microsoft, які стали технологічними гігантами.

– соціальні зміни: Зростання цифрових платформ, що інтегрують фізичний і цифровий світи (наприклад, розумні міста, автоматизовані транспортні системи, онлайн-освіта).

Ці етапи відображають еволюцію Інтернету, який з інструменту для наукових досліджень перетворився на всесвітню інформаційну та комунікаційну інфраструктуру, що значно змінила економічні, соціальні та культурні процеси в світі [76].

При розгляді можливостей Мережі в галузі публічного управління слід, на наш погляд, в першу чергу звернути увагу на такі обставини:

1. Забезпечення доступу до інформації – Мережа може значно полегшити доступ громадян до важливої публічної інформації, сприяючи прозорості діяльності органів державної влади та місцевого самоврядування. Відкритість даних дозволяє ефективніше відстежувати виконання політичних рішень, програм та проектів.

2. Участь громадян у процесах управління – Використання Мережі дозволяє громадянам активніше брати участь у процесах прийняття рішень, обговорення політик, вираження своїх думок та пропозицій щодо розвитку країни чи регіону. Це створює можливості для прямої демократії, де громадяни можуть мати реальний вплив на формування політики.

3. Зниження бюрократичних бар'єрів – Застосування цифрових платформ для подачі документів, заявок, скарг тощо дозволяє значно спростити бюрократичні процеси. Це робить взаємодію між державними органами та громадянами більш ефективною та зручнішою.

4. Інновації в управлінні та координації – Мережа може стати потужним інструментом для інтеграції різних державних і громадських структур, що дозволить швидше реагувати на змінювані ситуації, полегшити комунікацію між міністерствами, місцевими органами влади та іншими учасниками публічного управління.

5. Підвищення ефективності державних послуг – Впровадження цифрових технологій та мережевих рішень дозволяє оптимізувати надання

державних послуг, скоротити час на їх отримання та знизити витрати як для держави, так і для громадян.

6. Безпека та захист даних – Враховуючи обсяг інформації, що обробляється через Мережу, особливу увагу слід приділити питанням безпеки даних, захисту конфіденційної інформації та протидії кіберзагрозам. Створення надійних механізмів захисту інформації є критично важливим для забезпечення довіри громадян до цифрових платформ публічного управління.

7. Інклюзивність та доступність – Необхідно забезпечити, щоб цифрові технології були доступні для всіх громадян, включаючи ті категорії, які можуть мати обмежений доступ до інтернету чи цифрових платформ. Це дозволить забезпечити рівність в доступі до публічних послуг та інформації.

Розглядаючи ці аспекти, можна визначити, як Мережа може стати потужним інструментом для розвитку публічного управління, покращення взаємодії між державою та громадянами, а також сприяти більш ефективному управлінню на всіх рівнях.

Комунікаційні можливості Мережі відіграють критичну роль у сучасному публічному управлінні, особливо в умовах гібридних загроз. Гібридні загрози, що включають кібератаки, дезінформацію, маніпуляції через соціальні медіа та інші форми нелінійної війни, ставлять серйозні виклики для функціонування державних і публічних інституцій, а також для забезпечення безпеки інформаційного простору [76].

Важливі аспекти, на які слід звернути увагу при дослідженні комунікаційних можливостей Мережі в умовах гібридних загроз:

1. Захист інформаційної інфраструктури

У разі гібридних загроз, важливо мати надійні технічні засоби, які забезпечують захист від кібератак. Це можуть бути:

– системи кібербезпеки, що здатні виявляти та запобігати атакам, в тому числі DDoS-атакам, фішингу, malware, та іншим шкідливим програмам.

– шифрування даних для захисту інформації від несанкціонованого доступу, особливо в умовах конфіденційної комунікації між органами влади та громадянами.

– аутентифікація і багатофакторний доступ до державних онлайн-ресурсів для забезпечення надійного доступу та обмеження можливостей для зловмисників.

2. Моніторинг та реагування на дезінформацію

Гібридні загрози часто включають кампанії з дезінформації, що можуть маніпулювати громадською думкою. Важливо розробити ефективні механізми моніторингу та виявлення фальшивих новин або пропагандистських матеріалів у Мережі, а також способи своєчасної реакції на них:

– автоматизовані системи моніторингу для виявлення та аналізу медіа-контенту на наявність фейків або маніпуляцій.

– співпраця з незалежними медіа та фактчекерами, які допомагають верифікувати інформацію.

– платформи для швидкого реагування, які можуть виправляти або спростовувати недостовірну інформацію в режимі реального часу.

3. Зручність та оперативність доступу до інформації

Іншою важливою складовою є забезпечення зручного і швидкого доступу до правдивої та актуальної інформації для громадян та державних структур:

– інтерактивні платформи та додатки, що надають зручний доступ до публічних послуг, повідомлень про безпеку, а також інформації про державну політику та інші важливі питання.

– мобільні додатки та системи оповіщення, що дозволяють у реальному часі отримувати важливі новини або аварійні повідомлення.

– доступність на різних платформах (інтернет, мобільні телефони, телебачення) для забезпечення безперебійного доступу до інформації незалежно від технологічних можливостей громадян.

4. Відновлення комунікацій в умовах кризових ситуацій

У разі виникнення гібридних атак, які можуть призвести до відключення частини інформаційних або комунікаційних мереж, важливо мати на увазі такі заходи:

– резервні канали зв'язку, які можуть забезпечити продовження комунікації, навіть якщо основні канали будуть заблоковані або знищені.

– механізми відновлення після кібератак та інші заходи для відновлення функціонування інформаційних систем і забезпечення доступу до важливої інформації.

5. Підвищення рівня цифрової грамотності

Оскільки в умовах гібридних загроз важлива роль належить саме користувачам інформаційних технологій, необхідно забезпечити підвищення цифрової грамотності серед населення:

– освітні програми та тренінги для населення щодо безпеки в інтернеті, розпізнавання фейкових новин і запобігання кібератакам.

– навчання державних службовців з питань кібербезпеки та безпечної роботи з публічною інформацією.

6. Інклюзивність технологічних засобів

Технічні засоби, які використовуються для комунікації з громадянами, мають бути інклюзивними. Це означає:

– підтримка різних мовних версій інформаційних платформ для забезпечення доступу до інформації для всіх соціальних груп.

– адаптація для осіб з інвалідністю, наприклад, через використання аудіо- та відео матеріалів для людей з обмеженнями слуху чи зору.

Таким чином, технічні засоби та комунікаційні можливості Мережі не лише сприяють зручному доступу до публічної інформації, але й забезпечують протидію гібридним загрозам, зберігаючи стабільність та безпеку публічного управління в умовах глобальних викликів.

3.2 Використання сучасних знарядь щодо інформаційного забезпечення публічного управління

Використання нових інструментів в інформаційному забезпеченні публічного управління є важливим аспектом модернізації державних інститутів, спрямованим на підвищення ефективності та прозорості управлінських процесів. Застосування сучасних технологій дозволяє забезпечити швидший доступ до інформації, знижує витрати, покращує взаємодію з громадянами та підвищує якість прийняття рішень [54].

Ось деякі з основних інструментів, які активно використовуються в публічному управлінні:

Електронне урядування включає в себе використання інформаційно-комунікаційних технологій (ІКТ) для покращення управлінських процесів, а також забезпечення доступу громадян до державних послуг через інтернет. Це може включати:

– електронні державні послуги: надання різноманітних послуг онлайн, таких як реєстрація бізнесу, подання податкових декларацій, отримання ліцензій, реєстрація автомобілів тощо.

– цифрові платформи для взаємодії з громадянами: створення онлайн-майданчиків для подачі звернень, відстеження статусу документів, голосування чи участі в опитуваннях.

Аналіз великих обсягів даних дозволяє органам публічного управління:

– прогнозувати потреби громадян: аналіз даних може допомогти виявити тренди та прогнозувати майбутні проблеми, такі як зростання попиту на медичні послуги або необхідність у житлових приміщеннях.

– оптимізувати ресурси: використання даних для більш ефективного розподілу ресурсів, наприклад, у сфері охорони здоров’я чи транспорту.

– покращити прийняття рішень: аналіз даних допомагає формувати більш обґрунтовані рішення на основі об'єктивної інформації.

Блокчейн технології забезпечують прозорість і безпеку в управлінні державними процесами:

– прозорість у публічних фінансах: використання блокчейну для відслідковування державних витрат, що знижує ризик корупції.

– електронний документообіг: блокчейн дозволяє зберігати документи без можливості їх змінювати або фальсифікувати, що забезпечує надійність та прозорість адміністративних процесів.

– електронні вибори: блокчейн може забезпечити безпечне і прозоре проведення виборів, зменшуючи ризик маніпуляцій.

Інтернет речей дозволяє підвищити ефективність управлінських процесів завдяки постійному збору даних з різноманітних сенсорів і пристроїв:

– розумні міста: застосування IoT для моніторингу інфраструктури, транспорту, енергоспоживання, безпеки тощо. Наприклад, датчики на вулицях можуть виявляти проблеми з освітленням, заторами або забрудненням повітря.

– моніторинг стану навколишнього середовища: використання IoT для збору даних про якість води, повітря, температуру і вологість для забезпечення кращого управління природними ресурсами.

Штучний інтелект та машинне навчання використовуються для автоматизації та покращення процесів прийняття рішень:

– автоматизація адміністративних процесів: штучний інтелект може допомогти в автоматизації рутинних завдань, таких як обробка запитів громадян, перевірка документації, аналіз податкових декларацій.

– антифрод-системи: ШІ може виявляти аномалії та шахрайські схеми в публічних фінансах, забезпечуючи додатковий рівень безпеки.

– поліпшення обслуговування громадян: чат-боти та віртуальні асистенти можуть допомогти автоматизувати відповіді на запити громадян, що значно зменшує час очікування та покращує доступ до послуг.

Сучасні цифрові платформи надають можливість громадянам брати активну участь у процесах прийняття рішень:

– онлайн-консультації та опитування: органи державної влади можуть проводити консультації з громадськістю, щоб отримати зворотній зв'язок щодо політик чи законопроєктів.

– платформи для подачі петицій та звернень: громадяни можуть подавати електронні петиції чи звернення до органів влади, що стимулює діалог і покращує зворотний зв'язок між владою і громадянами.

Мобільні додатки, створені для забезпечення доступу до державних послуг, стали дуже популярними:

– мобільний доступ до послуг: додатки, через які можна отримати інформацію про стан документів, записатися на прийом до лікаря, оплатити штрафи тощо.

– push-сповіщення: громадяни отримують актуальну інформацію через мобільні сповіщення (наприклад, про зміни в законодавстві чи терміни подання звітності).

Використання нових інформаційних інструментів в публічному управлінні сприяє значному покращенню ефективності, прозорості та доступності управлінських процесів. Це дозволяє державним органам оперативніше реагувати на зміни в суспільстві та економіці, підвищувати рівень довіри громадян до органів влади та забезпечувати більш високий рівень обслуговування громадян. Водночас важливо забезпечити захист персональних даних і безпеку інформаційних систем для уникнення можливих ризиків та зловживань.

Перспективи ефективного використання Інтернету в публічному управлінні пов'язані здебільшого з вирішенням низки ключових питань, що стосуються як технологічних, так і організаційних аспектів [39]. Ось кілька таких важливих питань:

Одним з найбільших викликів є перехід від традиційних паперових процесів до електронних. Для цього необхідно:

– створення інтегрованих електронних платформ для автоматизації рутинних адміністративних процедур (реєстрація бізнесу, надання дозволів, оформлення соціальних виплат тощо).

– розробка та впровадження електронних підписів, що забезпечать легітимність та юридичну силу електронних документів.

– оцифрування архівів та документів для зручності їх доступу та обробки.

Оскільки Інтернет-ресурси в публічному управлінні зберігають і обробляють великі обсяги персональних та конфіденційних даних, важливо:

– розробити та впровадити ефективні системи кібербезпеки, що забезпечують захист від кіберзагроз, таких як хакерські атаки або витоки інформації.

– використовувати новітні технології шифрування для збереження конфіденційності даних.

– забезпечити відповідність національним та міжнародним стандартам захисту персональних даних, зокрема у відповідності до GDPR (Загальний регламент захисту даних) або аналогічних стандартів.

Потрібно підвищити рівень цифрової грамотності як серед громадян, так і серед державних службовців:

– розробка освітніх програм для громадян, що допоможуть їм зрозуміти, як ефективно користуватися онлайн-державними послугами.

– навчання державних службовців для того, щоб вони могли оперативно реагувати на запити громадян через Інтернет, а також ефективно використовувати нові технології для автоматизації внутрішніх процесів.

– програмування курсів для покращення навичок роботи з новими цифровими інструментами та платформами, що полегшать повсякденну роботу держслужбовців.

Одним з основних завдань для органів публічного управління є підвищення прозорості їхньої діяльності [80]. Для цього:

– необхідно відкривати дані, що стосуються витрат бюджету, публічних закупівель, проектів і програм державного фінансування (відкриті дані).

– створення платформ для громадського контролю, де громадяни можуть відслідковувати, як витрачаються державні кошти або як приймаються управлінські рішення.

– створення онлайн-ресурсів для подання петицій, опитувань та обговорень важливих політичних чи соціальних питань, що дає змогу громадянам брати активну участь у процесах управління.

Для підвищення ефективності взаємодії між різними державними органами та з громадянами потрібно забезпечити інтеграцію різних інформаційних систем:

– розробка єдиних порталів для надання всіх основних електронних послуг в одному місці (наприклад, реєстрація бізнесу, подача податкових декларацій, отримання дозволів, оформлення соціальних виплат).

– інтеграція систем для обміну даними між державними органами на різних рівнях, щоб забезпечити швидкий доступ до необхідної інформації для прийняття рішень (наприклад, між міністерствами, місцевими органами влади та підприємствами).

– використання модульних систем, які дозволяють адаптувати та розширювати інструменти в залежності від потреб.

Сучасні цифрові комунікаційні канали, такі як соціальні медіа, чат-боти, мобільні додатки, можуть значно покращити взаємодію між державою та громадянами:

– використання соціальних мереж для оголошення важливої інформації, анонсування нових послуг або змін у законодавстві, а також для взаємодії з громадянами у реальному часі.

– впровадження чат-ботів та віртуальних асистентів, що можуть допомогти громадянам отримати відповіді на поширені запитання,

направляти їх до потрібних ресурсів або навіть реєструвати заяви та звернення.

– мобільні додатки, через які громадяни можуть отримати доступ до публічних послуг, перевірити статус запитів чи отримати повідомлення про важливі події.

Потрібно забезпечити, щоб усі громадяни мали рівний доступ до електронних послуг, включаючи людей з обмеженими можливостями:

– розробка інклюзивних інтерфейсів для вебсайтів і мобільних додатків, що забезпечують доступність для людей з інвалідністю (наприклад, підтримка екранних читалок, можливість зміни контрасту та шрифтів).

– доступність послуг для всіх соціальних груп: врахування потреб різних верств населення, у тому числі людей з обмеженим доступом до Інтернету або з низьким рівнем цифрових навичок.

Для забезпечення ефективного управління необхідно покращити координацію між центральними, регіональними та місцевими органами влади:

– розробка спільних платформ для обміну даними та комунікації між органами різних рівнів.

– забезпечення єдиного стандарту для електронних документів, щоб органи на всіх рівнях могли безперешкодно обмінюватися інформацією.

Важливим аспектом є постійний моніторинг та оцінка ефективності електронних послуг:

– оцінка використання онлайн-ресурсів: аналіз статистики користування вебсайтами та платформами для визначення, наскільки зручними є ці ресурси для громадян.

– збір відгуків від користувачів для вдосконалення онлайн-ресурсів та виявлення потенційних проблем або недоліків.

Перспективи ефективного використання Інтернету в публічному управлінні включають вирішення цілої низки завдань, пов'язаних із цифровізацією адміністративних процесів, підвищенням безпеки,

забезпеченням прозорості, підвищенням цифрової грамотності громадян та службовців, інтеграцією систем та інклюзивністю [75]. Рішення цих питань дозволить значно покращити якість та доступність державних послуг, а також підвищити рівень довіри громадян до органів публічного управління.

Підвищення ефективності використання Інтернет-ресурсів органами державної влади усіх рівнів є важливим кроком до модернізації публічного управління, сприяння прозорості та доступності державних послуг для громадян [77]. Інтернет-ресурси включають сайти органів влади, соціальні медіа, мобільні додатки, електронні платформи для взаємодії з громадянами та інші цифрові інструменти, що забезпечують доступ до інформації та послуг. Ось кілька ключових аспектів підвищення ефективності використання Інтернет-ресурсів органами державної влади:

Поліпшення доступності та зручності користування: Інтуїтивно зрозумілий інтерфейс: Вебсайти органів влади мають бути зручними для користувачів. Вони повинні мати просту навігацію, чітко структуровану інформацію та можливість швидкого пошуку потрібних даних. Адаптивний дизайн: вебсайти повинні бути адаптовані для мобільних пристроїв, оскільки все більше громадян використовують смартфони для доступу до державних послуг. Мультиканальність: надання однакових послуг через кілька каналів — вебсайт, мобільний додаток, чат-боти, соціальні мережі — дозволяє зручніше взаємодіяти з громадянами з урахуванням їхніх вподобань.

Електронні послуги та автоматизація процесів: Цифровізація адміністративних процедур: Перехід від паперових форм до електронних — це значний крок до спрощення процедур. Наприклад, можливість онлайн подати документи, оформити заяви чи запити. Автоматизація прийняття рішень: використання цифрових інструментів для автоматизації рутинних завдань (наприклад, обробка заявок на отримання ліцензій або дозвільних документів) зменшує навантаження на працівників державних органів і прискорює процеси. Цифрові платформи для надання послуг: створення єдиних платформ, де громадяни можуть отримувати різні адміністративні

послуги (наприклад, онлайн реєстрація бізнесу, отримання медичних довідок, запити на субсидії).

Покращення комунікації та взаємодії з громадянами [29]. Соціальні медіа та онлайн-платформи: Використання соціальних мереж для комунікації з громадянами дає змогу швидко реагувати на запити та питання. Влада може використовувати платформи як Facebook, Twitter, Instagram для оголошень, важливих новин або консультацій. Онлайн-консультації та зворотний зв'язок: Органи влади можуть організовувати онлайн-консультації або вебінари з громадянами, щоб обговорити актуальні питання або політики. Це також може бути формою громадських слухань чи участі в розробці нових законів. Чат-боти та віртуальні асистенти: Віртуальні помічники можуть автоматично відповідати на найбільш поширені запитання, допомагати у навігації по вебсайту, а також надавати інформацію про статус поданих заяв [9].

Прозорість і відкритість інформації. Відкриті дані (Open Data): Публікація відкритих даних у форматах, зручних для аналізу (наприклад, CSV, JSON), дозволяє громадянам і підприємствам отримувати доступ до інформації про державні витрати, статистику, закупівлі та інші аспекти діяльності органів влади. Прозорість у фінансах: Онлайн-системи для моніторингу використання публічних коштів дозволяють відслідковувати, як витрачаються бюджетні кошти, що підвищує довіру громадян до органів влади. Інтерфейси для звернень: Створення простих платформ для подачі звернень та петицій, через які громадяни можуть звертатися до органів влади з різними запитами, ініціативами чи скаргами. Це підвищує рівень зворотного зв’язку.

Інтеграція та взаємодія між різними органами влади [4]. Єдині цифрові платформи для взаємодії: Розробка інтегрованих електронних платформ для обміну даними між різними рівнями влади (місцевим, регіональним, центральним). Це дозволяє скоротити бюрократичні процедури та підвищити швидкість обробки запитів. Інтеграція баз даних: Органи державної влади можуть інтегрувати свої бази даних, що дозволяє уникнути дублювання

інформації, підвищити точність і швидкість обробки заяв, а також зменшити адміністративні бар'єри для громадян.

Забезпечення безпеки і захисту даних. Захист персональних даних: З ростом використання цифрових інструментів дуже важливим є забезпечення захисту персональної інформації громадян. Органи державної влади повинні відповідати національним і міжнародним стандартам щодо безпеки даних. Аутентифікація та верифікація: Використання безпечних способів аутентифікації громадян на електронних платформах, наприклад, через цифрові підписи, банківські ідентифікації, системи е-ідентифікації (наприклад, через застосунок "Дія") [40].

Освіта та підвищення кваліфікації державних службовців. Навчання державних службовців: Важливо, щоб посадові особи органів влади мали належні навички для роботи з новими інтернет-ресурсами. Тому постійне навчання та підвищення кваліфікації в цих питаннях є необхідним. Покращення цифрових компетенцій: Потрібно створювати програми підвищення цифрової грамотності для державних службовців, щоб вони могли ефективно працювати з новими технологіями та забезпечувати високий рівень послуг громадянам.

Підвищення ефективності використання Інтернет-ресурсів органами державної влади сприяє покращенню управлінських процесів, підвищенню рівня взаємодії між владою та громадянами, а також забезпеченню прозорості та доступності послуг. Це дозволяє зменшити адміністративні бар'єри, прискорити процеси, підвищити рівень довіри до державних органів і зробити публічне управління більш ефективним.

3.3 Розроблення напрямів застосування засобів мережі Internet у системі публічного управління в умовах гібридних загроз

В умовах гібридних загроз використання Інтернет-ресурсів в публічному управлінні має особливе значення для забезпечення стабільності

та безпеки державних інститутів, а також підтримки ефективної взаємодії між органами влади та громадянами. Гібридні загрози включають не тільки традиційні військові загрози, але й кібератаки, інформаційні війни, дезінформацію, психологічні операції та інші форми маніпуляцій. Тому стратегія розвитку основних інформаційних ресурсів повинна враховувати забезпечення кібербезпеки, прозорості, доступності та ефективної комунікації [53].

Функціональна схема розвитку основних інформаційних ресурсів в умовах гібридних загроз/

Розбудова національної інфраструктури кібербезпеки. Основні напрямки: підвищення рівня кіберзахисту органів публічного управління.

– впровадження сучасних систем кіберзахисту для захисту від кібератак, зокрема DDoS-атак, фішингу, атак на бази даних.

– впровадження багаторівневої системи автентифікації та шифрування для забезпечення безпеки комунікацій і обміну даними.

– створення національного центру кібербезпеки.

– цей центр буде координувати діяльність органів влади щодо запобігання та реагування на кіберзагрози, проводити регулярні тренування для державних службовців.

– розробка і впровадження стратегії збереження даних.

– встановлення стандартів для резервного зберігання даних, розподілених серверів і хмарних технологій з урахуванням загроз кібератак.

Використання систем для боротьби з інформаційними загрозами. Основні напрямки:

– моніторинг і блокування дезінформації.

– створення спеціалізованих систем моніторингу для виявлення та оперативного реагування на інформаційні маніпуляції, фальшиві новини та ворожу пропаганду в Інтернеті.

– платформи для спростування фейкових новин.

– створення єдиної платформи для швидкого спростування фейкових новин, де державні органи та незалежні експерти можуть надавати достовірну інформацію.

– використання ШІ для виявлення пропаганди.

– розробка алгоритмів на основі штучного інтелекту, що дозволяють автоматично виявляти пропагандистські матеріали в Інтернеті та соцмережах.

Цифрові платформи для посилення взаємодії між владою і громадянами. Основні напрямки:

– електронне урядування (e-Government).

– розвиток інтегрованих цифрових платформ для надання адміністративних послуг (податкова звітність, реєстрація бізнесу, видача дозволів тощо), що дозволяє мінімізувати фізичний контакт з державними органами та знижує ризики корупції.

– мобільні додатки для державних послуг.

– розробка мобільних додатків для доступу до всіх основних публічних послуг, зокрема через додатки типу "Дія", що дають змогу громадянам отримати електронні документи, послуги в один клік.

– прозорість і підзвітність.

– платформи для публікації даних про використання публічних коштів, виконання державних контрактів, моніторинг витрат бюджету, що дозволяє громадянам контролювати діяльність органів влади.

Інтеграція різних інформаційних систем. Основні напрямки:

– інтеграція баз даних.

– створення єдиної платформи для обміну даними між різними державними органами на всіх рівнях (місцевому, регіональному, центральному) для швидшого прийняття рішень.

– інтеграція з приватними компаніями.

– взаємодія з приватним сектором через відкриті API та цифрові платформи для забезпечення прозорості у державних закупівлях та наданні послуг (наприклад, інтеграція банківських сервісів для онлайн-платежів).

– єдині портали для громадян.

– створення єдиного порталу для доступу до всіх державних послуг, через який громадяни зможуть подавати заявки, отримувати консультації та слідкувати за статусом своїх справ.

Системи для моніторингу та аналізу ризиків. Основні напрямки:

– системи прогнозування загроз.

– використання великих даних (Big Data) та штучного інтелекту для виявлення потенційних загроз в режимі реального часу (зокрема кіберзагроз, соціальних хвиль протестів, політичної дестабілізації).

– аналіз вразливостей національної інфраструктури.

– створення систем для постійного моніторингу вразливостей національних IT-ресурсів та інфраструктури публічного управління з метою своєчасного виявлення загроз та оперативного реагування.

6. Розвиток мобільних і хмарних технологій для оптимізації роботи державних органів. Основні напрямки:

– мобільні та хмарні платформи для держслужбовців.

– розвиток мобільних та хмарних сервісів для полегшення доступу до службових даних, документів та реєстраційних форм, що забезпечує швидке прийняття рішень і ефективність адміністративних процедур.

– безпечний доступ до даних з будь-якого пристрою.

– використання хмарних технологій для зберігання та доступу до інформації з мобільних пристроїв, забезпечуючи зручність роботи для держслужбовців у будь-яких умовах, з урахуванням безпеки.

Навчання та підвищення кваліфікації персоналу. Основні напрямки:

– цифрові курси для держслужбовців.

– впровадження онлайн-курсів для підвищення цифрової компетентності державних службовців і надання їм інструментів для ефективної роботи з Інтернет-ресурсами.

Функціональна схема розвитку основних інформаційних ресурсів в публічному управлінні з урахуванням існуючих напрямків застосування Інтернету може включати три основні складові: ресурси керівництва профільного міністерства, інформаційно-аналітичний центр і центральний WEB-сервер [34]. Ця схема повинна бути спрямована на забезпечення ефективного управління, збереження безпеки інформації, забезпечення доступу до послуг і ресурсів для громадян та організацій, а також оперативне реагування на гібридні загрози.

Функціональна схема розвитку основних інформаційних ресурсів

1. Ресурси керівництва профільного Міністерства.

Основні функції:

– стратегічне управління та прийняття рішень.

– платформи для збору, обробки та аналізу даних, що використовуються для прийняття рішень на рівні міністерства. Вони дозволяють об'єднувати інформацію з усіх підрозділів та інституцій в рамках державної політики.

– аналіз та моніторинг поточної ситуації.

– інформаційно-аналітичні системи, які збирають, обробляють і аналізують дані щодо виконання планів і програм, стану економіки, безпеки, соціальних питань.

– веб-ресурси для аналізу результатів публічних закупівель, використання бюджетних коштів, моніторингу ефективності державних послуг та прогресу в реалізації державних ініціатив.

– комунікація та взаємодія з громадянами і іншими державними органами.

– веб-сайти міністерства як основні канали для інформування громадян про політики, заходи, а також можливість онлайн-консультацій, опитувань та зворотного зв'язку.

– взаємодія через соціальні мережі та мобільні додатки для обміну інформацією, що дозволяє оперативно реагувати на запити та питання громадян.

Основні компоненти:

– інтерфейс для керівництва міністерства, що включає доступ до:

– статистичних і аналітичних даних.

– рішень, постанов та розпоряджень.

– оцінки виконання програми/проектів.

– система для стратегічного планування та звітності.

– використання інструментів для збору, обробки та надання звітів про виконання завдань.

2. Інформаційно-аналітичний центр

Основні функції:

– збір і обробка даних.

– центр відповідає за збір даних з різних джерел (веб-сайтів, відкритих даних, даних з інших державних установ) та їх централізовану обробку для формування аналітичних матеріалів для міністерства.

– постійний моніторинг змін в соціально-економічній ситуації, наявність нових загроз (глобальних та локальних), таких як кібератаки, інформаційні загрози, природні катастрофи, тощо.

– прогнозування і аналіз.

– використання систем прогнозування на основі великих даних (Big Data), що дозволяють визначити тенденції та передбачити майбутні виклики, зокрема для розвитку інфраструктури, державних послуг, економіки.

– оперативне реагування на інциденти та загрози.

– у разі виникнення гібридних загроз (наприклад, кібератак або інформаційних кампаній), центр забезпечує моніторинг і координує оперативну реакцію.

Основні компоненти:

– система збору та інтеграції даних.

– інтерфейси для збирання даних з різних джерел, включаючи дані відкритих джерел, спеціалізовані інформаційні платформи та внутрішні бази даних.

– аналітична платформа.

– інструменти для автоматичного аналізу даних, оцінки їх якості та формування звітів для вищих органів влади.

– моделі прогнозування.

– моделі для аналізу соціальних, економічних, політичних змін з урахуванням ризиків і можливих загроз.

3. Центральний WEB-сервер

Основні функції:

– інтеграція та доступ до інформаційних ресурсів.

– центральний сервер виступає як система управління контентом для зберігання та доступу до важливих державних даних (наприклад, дані про бюджет, нормативно-правові акти, відкриті дані) та забезпечує доступ до цих ресурсів для органів державної влади та громадян.

– платформа для публічного доступу до інформаційно-аналітичних матеріалів та звітування.

– безпека та захист даних.

– центральний сервер має забезпечувати високу безпеку зберігання даних (зокрема, персональних даних), їх шифрування та захист від зовнішніх кіберзагроз. Всі взаємодії через центральний сервер повинні бути захищені за допомогою механізмів криптографії.

– мобільний доступ і інтеграція з іншими ресурсами.

– зручність і доступність ресурсів через мобільні додатки, що дозволяють громадянам звертатися за електронними послугами та взаємодіяти з органами влади.

– інтеграція з іншими державними реєстрами та базами даних для безперешкодного обміну даними між органами влади та забезпечення виконання адміністративних процедур.

Основні компоненти:

– система управління контентом (CMS).

– забезпечення зберігання та пошуку інформації за різними критеріями (законодавчі акти, звіти, статистика, бюджетні документи).

– інтерфейс для адміністрування доступу.

– керування доступом до конфіденційної та публічної інформації для державних органів та громадян, відповідно до їхніх прав.

– механізми резервного копіювання та відновлення даних.

– забезпечення стабільної роботи веб-платформ з регулярним збереженням і відновленням даних у разі інцидентів або атак.

Загальна функціональна схема

Міністерство (Ресурси керівництва)

– стратегічне управління, прийняття рішень

– аналітика та моніторинг

– взаємодія з іншими органами та громадянами

Інформаційно-аналітичний центр

– збір, обробка, аналіз даних

– прогнозування та моніторинг ризиків

– оперативне реагування на загрози

Центральний WEB-сервер

– інтеграція даних, доступ до інформаційних ресурсів|

– безпека, захист даних

– мобільний доступ і інтеграція з іншими платформами|

Ця схема розвитку основних інформаційних ресурсів у публічному управлінні в умовах гібридних загроз має забезпечити інтеграцію всіх необхідних компонентів для ефективного управління державними ресурсами, швидкого реагування на інформаційні загрози та забезпечення прозорості в діяльності органів державної влади. Важливими аспектами є забезпечення безпеки, моніторинг і аналіз поточної ситуації, а також забезпечення доступу громадян до електронних послуг в умовах гібридних загроз.

ВИСНОВКИ

1. Роботі обґрунтовано основи інформаційного забезпечення системи публічного управління в умовах гібридних загроз. Інформаційне забезпечення системи публічного управління в умовах гібридних загроз є важливою складовою забезпечення національної безпеки та ефективності управління в умовах постійно змінюваного політично-соціального середовища, в якому одночасно реалізуються як традиційні, так і новітні загрози. Інформаційне забезпечення системи публічного управління в умовах гібридних загроз є ключовим елементом забезпечення державної безпеки, стабільності та ефективності управлінських процесів. Воно вимагає інтеграції новітніх інформаційних технологій, активного захисту інформаційних ресурсів, боротьби з дезінформацією та постійного вдосконалення інформаційної політики на всіх рівнях управління.

2. Вплив комунікаційного менеджменту та маркетингу послуг на інформаційне забезпечення системи публічного управління в умовах гібридних загроз є значущим, оскільки ці сфери допомагають формувати ефективну комунікацію між державою та громадянами, а також забезпечують належну інформаційну безпеку та управлінську прозорість у кризових ситуаціях. В умовах гібридних загроз, таких як інформаційні війни, кібернапади або дезінформація, ці інструменти можуть стати вирішальними для стабільності суспільства та функціонування публічного управління. Інтеграція комунікаційного менеджменту та маркетингу послуг має значний вплив на інформаційне забезпечення публічного управління в умовах гібридних загроз. Вони допомагають створити ефективну систему комунікації між державними органами та громадянами, що є необхідною умовою для протидії кризам, збереження соціальної стабільності та забезпечення національної безпеки.

3. Аналіз стану застосування інформаційних технологій у побудові аналітично-інформаційного забезпечення функціонування публічних органів

влади показав, що інформаційні технології (ІТ) відіграють вирішальну роль у функціонуванні публічних органів влади, оскільки вони сприяють підвищенню ефективності управлінських процесів, забезпечують прозорість діяльності влади, а також дозволяють швидко реагувати на зовнішні та внутрішні виклики. Однією з ключових складових сучасного публічного управління є аналітично-інформаційне забезпечення, яке включає системи збору, обробки та аналізу даних, що допомагають органам влади ухвалювати обґрунтовані рішення на всіх рівнях управління. Інформаційні технології значно покращили аналітико-інформаційне забезпечення діяльності публічних органів влади, забезпечивши більш ефективну, прозору та швидку взаємодію з громадянами та між державними установами. Однак для максимізації цих переваг необхідно вирішити ряд викликів, зокрема забезпечення кібербезпеки, усунення цифрового розриву та створення належного кадрового потенціалу для підтримки таких технологій.

4. Дослідження сучасного стану впровадження інформаційного забезпечення інформаційних технологій у системі публічного управління міста Харкова в умовах гібридних загроз показало, що місто Харків, як одне з найбільших і найважливіших економічних, культурних і політичних центрів України, потребує ефективної і надійної інформаційної інфраструктури для забезпечення стабільного функціонування органів публічного управління. З початку війни в Україні в 2014 році, а зокрема після повномасштабного вторгнення Росії в 2022 році, Харків став важливим об'єктом, що знаходиться в умовах постійних гібридних загроз, таких як кібер-атаки, інформаційні операції, а також військові дії. У таких умовах ефективне використання інформаційних технологій (ІТ) для забезпечення функціонування публічної адміністрації стало критично важливим. Інформаційні технології стали ключовим елементом у публічному управлінні Харкова в умовах гібридних загроз. Місто активно розвиває цифрову інфраструктуру, зокрема через впровадження платформ для надання електронних послуг, покращення кібербезпеки та використання сучасних аналітичних систем. Однак для

подальшого розвитку необхідно зосередити увагу на зменшенні цифрового розриву, посиленому захисті від кіберзагроз і забезпеченні стійкості критичної інфраструктури в умовах війни.

5. В умовах гібридних загроз, що включають інформаційні війни, кібернапади, маніпуляції з громадською думкою та традиційні військові дії, публічне управління повинно бути готове до оперативних змін і адаптацій для забезпечення стабільності, ефективності та прозорості. Сучасні інформаційні технології (ІТ) можуть значно підвищити стійкість органів державної влади до таких загроз і допомогти в побудові більш ефективної системи управління. Ось кілька напрямів для впровадження ІТ у систему публічного управління в умовах гібридних загроз:

– розвиток та інтеграція інфраструктури кібербезпеки;

– впровадження технологій блокчейн для забезпечення прозорості та підзвітності;

– розвиток технологій для управління надзвичайними ситуаціями та кризовими явищами;

– інтеграція штучного інтелекту (ШІ) та аналітики великих даних;

– створення системи цифрової ідентифікації та безпечного доступу;

– розвиток мобільних платформ та додатків для громадян;

– інтеграція системи управління міським господарством та інфраструктурою (Smart City);

– розвиток партнерств із приватним сектором та міжнародними організаціями.

6. Застосування засобів Інтернету у системі публічного управління в умовах гібридних загроз є важливим елементом для забезпечення ефективного функціонування державних інститутів, зокрема у кризових або військових ситуаціях. У контексті гібридних загроз — це поєднання військових, політичних, економічних, інформаційних та інших методів впливу, — мережа Інтернет може служити як інструмент для швидкої комунікації, розповсюдження інформації, а також для боротьби з

інформаційними війнами та кібератаками. Ось основні напрямки застосування засобів Інтернету в публічному управлінні в умовах гібридних загроз: комунікація та взаємодія з громадянами; аналітика та моніторинг загроз; кібербезпека та захист інфраструктури; інформаційна війна та контрпропаганда; координація в рамках міжнародних та міжвідомчих відносин; цифровізація органів публічного управління; залучення громадян до процесів управління; резервні системи та відновлення після катастроф. Загалом, Інтернет в умовах гібридних загроз має як сильні, так і слабкі сторони. Водночас, він є потужним інструментом для забезпечення національної безпеки, публічного управління та ефективної комунікації, але потребує постійного розвитку в контексті забезпечення кібербезпеки та боротьби з інформаційними атаками.

7. Впровадження сучасних інформаційних технологій у систему публічного управління є необхідним кроком для забезпечення стійкості державних структур до гібридних загроз. ІТ-рішення можуть покращити ефективність управління, підвищити прозорість та підзвітність органів влади, а також забезпечити безпеку критичної інфраструктури та громадян. Водночас необхідно враховувати виклики кіберзахисту, необхідність адаптації до змінюваного зовнішнього середовища та розвитку нових технологій, що потребують комплексної інтеграції і адаптації в реальних умовах.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Аліулов Р.Р. Проблеми механізму публічного управління / Держава. 2020. № 3. С. 15-23.

2. Андронова О.А. Електронний уряд у Європі та світі / URL: http://www.ci.ua/inform22_01/p_06oo.htm

3. Арнольд В.І. Теорія катастроф. иїв Наука. 2021. С. 128.

4. Бакуменко В.Д. Формування державно-управлінських рішень: проблеми теорії, методології, практики: [монографія]. Київ: Вид-во УАДУ, 2016. 328 с.

5. Вайнштейн Г. Інтернет як фактор суспільних трансформацій / Світова економіка та міжнародні відносини. 2020. № 3. С. 19.

6. Василькова А. Порядок і хаос у розвитку соціальних систем / Київ. 132 с.

7. Вебер М. Мова для загальної інформації австрійських офіцерів у Відні (1918 р.) URL: http://www.soc.pu.ua:8101/publications/jssa/1999/3/3 weber.htmI.

8. Веймер Девід Л. Аналіз політики: Концепція і практика / [пер. з англ. Іван Дзюб, Анатолій Олійник; наук. ред. О. Кілієвич]. Київ: Основи, 2015. 654 с.

9. Возженко В.А. Національна безпека: теорія, політика, стратегія. Київ, 2019. 221 с.

10. Ворочек Х. Про стан «теорії маркетингу послуг» / Проблеми теорії та практики управління. 2020. № 2. С. 199.

11. Галкін С.Є. Бізнес у Інтернеті / Київ: 2022. 243 с.

12. Голобуцкий А. Електронний уряд URL: http://golob.narod.ua/egovper.

13. Голобуцький О. Концепція електронного урядування і сучасні потреби України / Політичний менеджмент. 2019. № 5 (16). С.15-16.

14. Публічне управління і менеджмент: [навч. посібник у таблицях і схемах] / Г.С. Одінцова, Г.І. Мостовий, О.Ю. Амосов та ін.; За заг. ред. д-ра

екон. наук, проф. Одінцової. Харків: ХарРІ УАДУ, 2014. 492 с.

15. Дєгтяр А.О. Державно-управлінські рішення: інформаційно-аналітичне та державних установне забезпеченн: [монографія] / Харків: Вид-во ХарРІНАДУ «Магістр», 2014. 224 с.

16. Дєгтяр А.О. Системний підхід у державному управлінні: методологічний аспект / Інноваційні технології та механізми публічного управління на регіональному рівні: Матеріали наук-практ, конф. Харків: Вид-во ХарРІ НАДУ «Магістр», 2017. С. 3-8.

17. Додонов О.Г. Архітектура автоматизованих інформаційно-аналітичних систем органів державної влади / Математичні машини і системи. 2019. № 3,4. С. 138-146.

18. Іванов В.М. Соціальні технології в сучасному світі/ Київ: Наука, 2019. 242 с.

19. Іванов В.М. Управлінська парадигма XXI ст. У 3-х т. Т. 1. Київ: 2018. 281 с.

20. Іноземців Ст. Експансія творчості – виклик економічної епосі / Поліс. 2019. № 6. С. 123.

21. Іноземців В.Л. Розколота цивілізація: Передумови та можливі наслідки постекономічної революції / Київ: Наука, 2021. С.

22. Ібрагімова І. Зв'язки з громадськістю як індикатор ефективності публічного управління та показник стану громадянського суспільства / Вісник НАДУ. - 2021 № 4 С. 27-34.

23. Ібрагімова І. Інформаційне суспільство та взаємодія влади з громадськістю: вимоги ефективності / Вісник НАДУ. 2020. № 1. С. 36-42.

24. Ільченко М. Як нам перегнати світових лідерів, не наздоганяючи їх? / Урядовий кур'єр, 2019. № 5 11 січня. С. 14.

25. Інтернет-пошук став головним джерелом інформації,13.02.2006. URL: http://www.ua-admin. com/uanet/ primary. php?only_ general= 1&for_print=1&addon=textcatalog&id=1781&cat=88

26. Канігін Ю.М. Інформатизація управління: соціальні аспекти/АН

УРСР. Ін-т соціології. Київ: Наук. думка, 2020. 2561с.

27. Катаєв С. Трансформація сучасного українського суспільства: постмодерністський контекст / URL: http://www.cvu.kiev.ua/lp/03lp99u/4_l.html.

28. Клименко І.В. Технології електронного врядування / Київ: Центр сприяння інституційному розвитку державної служби, 2021. – 292 с.

29. Климовицька Г.Ю. Інформаційно-аналітичне забезпечення управління підприємництвом в регіоні / Зб. наук. праць "Економіка, менеджмент, підприємництво". Луганськ: Східноукраїнський національний університет ім. Володимира Даля, 2019. № 11. С. 234-237.

30. Климовицька Г.Ю. Регіональні особливості інформаційно-аналітичного забезпечення управління підприємництвом Актуальні проблеми економіки. Київ: НАУ, 2015. № 2(32). С. 172-176.

31. Клімушін П.С. Технології автоматизації управління підприємством: [навч. посіб.] Харків: Вид-во ХарРІ НАДУ «Магістр», 2007. 150 с.

32. Колесніченко І. М. Розвиток електронного урядування в Україні: інституціональний аспект / Бізнес Інформ. - 2014. - № 3. - С. 52-57.

33. Колесникова К. О. Співвідношення державного управління та публічного адміністрування у процесі суспільної трансформації / Публічне управління: теорія та практика. - 2013. - Вип. 3. - С. 41-45.

34. Колодій А Процес деліберації як складова демократичного врядування / Демократичні стандарти врядування й публічного адміністрування. 2018. №1 С. 106-110.

35. Концепція розвитку електронного урядування в Україні / О. Баранов, М. Демкова, С. Дзюба, За ред. А.І. Семенченко, 2009р. 16 с.

36. Кудрявцев О. Ю. Електронне урядування уконтексті легітимації політичної влади; В.о. Харків. нац. пед. ун-т ім. Г. С. Сковороди. Харків: Б.в., 2015. 19 с.

37. Кудрявцев О. Ю. Електронне урядування у сучасному політикоадміністративному просторі: монографія / Харків. нац. ун-т міськ.

госп-ва. ім. О. М. Бекетова. Харків: ХНУМГ ім. О. М. Бекетова, 2016. 184 с.

38. Кульчій І. О. Проблеми та перспективи організації реформування системи державного управління в Україні / Державне управління: удосконалення та розвиток. 2013. № 4. URL: http://nbuv.gov.ua/UJRN/Duur_2013_4_4

39. Курко М. Н. Зміст державного управління (теоретико-правовий аспект) / Юридичний вісник. Повітряне і космічне право. 2020. 1. С. 36-40.

40. Куц Ю. О. Природа та сутність державного управління / Теорія та практика державного управління і місцевого самоврядування. 2013. №1. с. 35-40

41.Литвин Н. В. Впровадження електронного урядування як основа формування інформаційного суспільства / Міждисциплінарні дослідження актуальних проблем застосування інформаційних технологій в сучасному світі: зб. матеріалів V Всеукр. наук.-практ. конф. «Глушковські читання», Київ, 2016 р. 2016. С. 119-121.

42. Лойко Л. І. Інструменти, механізми та еволюція електронного урядування / Правова держава: Щорічник наукових праць. 2010. Вип. 21. С. 471-476.

43. Лугиня М. В. Розвиток концепції ефективності в державному управлінні: теоретико-прикладний аспект: дис. … канд. наук з держ. укр.: 25.00.01 / Лугиня Марина Вікторівна. Київ, 2016. 254 с.

44. Луценко С. Л. Моделі побудови інформаційного суспільства: порівняльний аналіз / Ефективність державного управління : зб. наук. пр.. – Львів: ЛРІДУ НАДУ, 2010. Вип. 25. С. 313-321.

45. Малишева Л. О. Електронній уряд як механізм реформування державного управління в інформаційному суспільстві / Вісник СевНТУ: зб. наук.пр. Серія: Політологія. 2011. Вип. 123/2011. С. 203-206.

46. Мартинюк, В. М. Інформаційне суспільство: теоретичне осмислення феномену / Стратегічні питання світової науки. 2012. С. 13-15.

47. Матвейчук Л. О. Електронне урядування: правовий аспект /

Інвестиції: практика та досвід. 2016. № 9. С. 8588.

48. Матієва Я. С. Електронний уряд в умовах інформаційного суспільства як чинник стратегії реформування державного управління / Науковий вісник Академії муніципального управління. Серія : Управління. - 2011. Вип. 4. С. 291-298.

49. Матієшин Л. Використання досвіду Польщі для впровадження еурядування в Україні / Інформація, комунікація, суспільство 2015: матеріали 4-ої Міжнародної наукової конференції ІКС-2015, 20–23 травня 2015 року, Україна, Львів, Славське / Національний університет "Львівська політехніка", Кафедра соціальних комунікацій та інформаційної діяльності. Львів: Видавництво Львівської політехніки. 2015. С. 148–149.

50. Мищишин В. І. Аналіз особливостей побудови систем електронного урядування в Україні / Вісник Національного університету "Львівська політехніка". 2011. № 699: Інформаційні системи та мережі. С. 164-175.

51. Міненко М. А. Трансформація системи державного управління в сучасні моделі регулювання суспільства / Державне управління: удосконалення та розвиток. 2013. № 6. URL: http://nbuv.gov.ua/UJRN/Duur_2013_6_3

52. Мєзєнцев А. В. Електронне урядування, електронна демократія – підходи до визначень / Теорія та практика державного управління. 2015. Вип. 1. С. 64-69.

53. Обушна Н. І. Публічне управління як нова модель організації державного управління в Україні: теоретичний аспект / Ефективність державного управління. 2015. Вип. 44(1). С. 53-63.

54. Оленцевич Н. В. Державно-приватне партнерство у розвинених країнах світу: досвід для України / Економічний аналіз. 2014. Т. 15(1). С. 134-143.

55. Омельченко А. В. Організаційно-правові засади недержавного управління зовнішньоекономічною діяльністю в Україні / Адвокат.2011. № 4.-С.19-22.

56. Осійчук М. Модернізація державного управління і розвиток персоналу (французький досвід) / Ефективність державного управління: збір. наук.праць. 2011. Вип. 27. С. 253-263.

57. Пасічник М.В. Механізми впровадження нового публічного менеджменту: досвід США / Державне управління: теорія та практика. – 2009. №1. URL: http://www.academy.gov.ua/ej/ej9/doc_pdf/Pasichnyk_MV.pdf.

58. Пахнін М. Л. Вплив інформаційного суспільства на розвиток системи публічного управління / Теорія та практика державного управління. - 2015. Вип. 4. С. 55-62.

59. Пилипишин В. П. Поняття та основні риси державного управління / Юридична наука і практика. 2011. № 2. С. 1014.

60. Попок А. Сучасні підходи до здійснення реформування державного управління: досвід зарубіжних країн / Вісник Національної академії державного управління. 2012. №2. С. 13-20.

61. Проект навчального посібника «Концепцептуальні засади розвитку електронного урядування в Україні» / За ред. А.І. Семенченко, 2019 р. 82с.

62.. Радзієвський І. А. Трансформація системних характеристик державного управління в умовах глобалізації : автореф дис. на здобуття наук. Ступеня канд. наук з держ. упр. Спец. 25.00.01 «Державне управління» / І. А. Радзієвський . Київ, 2007. 16 с.

63. Решота О. А. Вдосконалення державного управління України із використанням досвіду зарубіжних країн: проблеми та перспективи / Ефективність державного управління : зб. наук.праць. Львів: ЛРІДУ НАДУ. 2009. С. 187-193.

64. Розвиток системи управління в ЄС: досвід для України: наук.розробка / за заг. ред. О. Я. Красівського. Київ: НАДУ, 2013. 56 с.

65. Савченко С. В. Еволюція переходу інформаційного суспільства в "суспільство знань" у добу глобалізації / Актуальні проблеми державного управління. 2020. № 2. С. 271-277.

66. Світлична А. В. Адміністративно-територіальна реформа: досвід

Польщі та напрацювання в Україні / Аспекти публічного управління. 2015. № 9. С. 20-25.

67. Світові моделі державного управління: досвід для України / за заг. ред. Ю. В. Ковбасюка, С. В. Загороднюка, П. І. Крайніка, Х. М. Дейнеги. Київ: НАДУ, 2012. 612 с.

68. Сергіна Т. В. Актуальні проблеми реалізації концепції розвитку електронного урядування в Україні / Електронна демократія: збір. наук.праць. 2021. URL: https://publicadministration.un.org.

69. Серенок А. О. Нормативно-правове забезпечення впровадження електронного урядування в Україні: ініціативи Президента України / Державне будівництво. 2015. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2015_1_7

70. Скалацький В. М. Концептуальні побудови та практичні моделі інформаційного суспільства / Гуманітарний часопис. 2012. № 4. С. 62–69.

71. Солових В. П. Становлення та загальна характеристика сучасних моделей державного управління / Публічне управління: теорія та практика. 2014. Вип. 1. С. 18-25.

72. Солових В. Традиційна (бюрократична) модель державного управління: концептуальний опис / Публічне управління: теорія та практика. 2014. Вип. 3. С. 5-9.

73. Солових В. П. "GOOD GOVERNANCE" як одна із сучасних моделей державного управління / Науковий вісник Академії муніципального управління. Серія : Управління. 2019. Вип. 1. С. 112-120.

74. Соловйов В. М. Новий державний менеджмент: визначення, сутність і ґенеза поняття / Вісник Київського національного університету імені Тараса Шевченка. 2020. № 1(1). С. 80 – 83.

75. Соловйов В. Особливості реформування державного управління Великобританії / Вісник Національної академії державного управління при Президентові України. 2010. Вип. 2. С. 38-46.

76. Соркін Б. В. Проблеми і перспективи розвитку державного

управління у сфері підприємництва в сучасній Україні / Наукові праці МАУП. 2014. Вип. 2(41). С. 71-75

77. Стрілець Ю. П. Принцип підконтрольності в контексті концепції "good governance" / Актуальні проблеми державного управління. 2011. № 2. С. 319-325.

78. Тильчик О. В. Особливості державного управління Федеративної республіки Німеччина та Польщі: досвід для України / Порівняльно-аналітичне право. 2015. №1. С. 223–226.

79. Ткач М.П. Проблеми визначення поняття державного управління / Правовий вісник Української академії банківської справи. 2020. № 1 (6). С. 60–65.

80. Чукут С. А., Кукарін О. Б Опорний конспект лекцій з курсу «Інформаційна політика та електронне урядування». Київ: Вид-но НАДУ, 2008. 98 с.

81. Шаповалова Н. Адміністративна реформа у Польщі: напрямки змін та реальні результати / URL: http://dialogs.org.ua/ru/cross/page3636.html.

82. Khaston Oan. «Marketing and Strategy». McGraw-Hill Publishing Company. 2020, 342p.