ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ГАЛУЗІ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ ТА ЇХ ВПЛИВ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ»

на здобуття освітнього ступеня магістр
за спеціальності 126 Інформаційні системи та технології
(код,найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Денис ТЕРЕЩЕНКО
(підпис) *(ім'я, ПРІЗВИЩЕ здобувача)*

Виконав:
здобувач вищої освіти
група ІСДМ-61 _____Денис ТЕРЕЩЕНКО_____
(ім'я, ПРІЗВИЩЕ)
Керівник __PhD___Валентина ДАНИЛЬЧЕНКО__
(ім'я, ПРІЗВИЩЕ)

Рецензент: _____
(ім'я, ПРІЗВИЩЕ)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інформаційних систем та технологій

Ступінь вищої освіти магістр

Спеціальність 126 Інформаційні системи та технології

Освітньо-професійна прорама Інформаційні системи та технології

ЗАТВЕРДЖУЮ

Завідувач кафедрою ІСТ

Каміла СТОРЧАК _____

“____” _____2025 року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Терещенку Денису Сепргійовичу

(прізвище, ім’я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Інформаційні технології в галузі публічного адміністрування та їх вплив на інформаційну безпеку

керівник кваліфікаційної роботи: Ваентина ДАНИЛЬЧЕНКО phD

(ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “___ ” жовтня 2025 р. № ____

2. Строк подання кваліфікаційної роботи «26» грудня 2025 р.

3. Вихідні дані кваліфікаційної роботи:

1. Технології Інтернет речей.

2. Архітектура IoT.

3. Методи виявлення аномалій і IoT.

4. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1. Дослідження тенденцій розвитку та поширення Інтернет речей.
2. Огляд методів виявлення аномалій в IoT.
3. Аналіз результатів впровадження моделі виявлення аномалій в IoT.

5.Перелік ілюстраційного матеріалу: презентація

6. Дата видачі завдання «___» _____ 2025р.

РЕФЕРАТ

У цьому дослідженні проаналізовано значення, яке мають нинішні інформаційні технології (ІТ) для еволюції системи державного адміністрування в Україні, а також їхній ефект на результативність державного сектору. Визначено провідні вектори цифрових перетворень, до яких належать електронне урядування, цифрова ідентифікація, залучення хмарних обчислень, робота з масивами великих даних (Big Data), застосування штучного інтелекту, а також нарощування обсягів відкритих даних у функціонуванні владних структур.

Ґрунтовно розглянуто українські зразки цифрової перебудови, а саме застосунок «Дія», систему електронної ідентифікації, ініціативи щодо захисту державних реєстрів від кібератак, та адаптовану для України платформу електронної взаємодії X-Road. З'ясовано, що інтеграція ІТ сприяє зростанню прозорості, зменшенню тягаря бюрократичних формальностей, покращенню доступу громадян до послуг та якіснішій комунікації між державою та її громадянами.

Сформульовано основні перешкоди, з якими стикається система публічного управління в Україні: наявність кібернетичних загроз, небезпеки несанкціонованого доступу до особистої інформації, застарілість ІТ-інфраструктури у певних відомствах, а також нерівномірність рівня володіння цифровими навичками серед населення. Наголошено на потребі зміцнення заходів інформаційної безпеки та оновлення відповідної законодавчо-нормативної бази.

Праця доводить, що ІТ виступають вирішальним каталізатором модернізації державного управління та його здатності відповідати сучасним викликам. Успішне переведення державних операцій у цифровий формат є визначальним для конкурентоспроможності держави та її інтеграції у світовий цифровий континуум.

КЛЮЧОВІ СЛОВА : ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ПУБЛІЧНЕ УПРАВЛІННЯ, ЦИФРОВА ТРАНСФОРМАЦІЯ, ЕЛЕКТРОННЕ УРЯДУВАННЯ, КІБЕРБЕЗПЕКА, ДЕРЖАВНІ ПОСЛУГИ, ВІДКРИТІ ДАНІ, ШТУЧНИЙ ІНТЕЛЕКТ, ХМАРНІ ТЕХНОЛОГІЇ, ДІЯ

ABSTRACT

This study analyzes the significance of modern information technologies (IT) for the evolution of the public administration system in Ukraine, as well as their impact on the effectiveness of the public sector. The key vectors of digital transformation are identified, including e-government, digital identification, the use of cloud computing, big data analytics, artificial intelligence, and the expansion of open data in the functioning of governmental institutions.

The research provides a detailed examination of Ukrainian examples of digital restructuring, namely the “Diia” application, the electronic identification system, initiatives aimed at protecting state registries from cyberattacks, and the X-Road electronic interoperability platform adapted for Ukraine. It is revealed that the integration of IT contributes to increasing transparency, reducing bureaucratic burdens, improving citizens’ access to services, and enhancing the quality of communication between the state and its citizens.

The main obstacles faced by Ukraine’s public administration system are identified: the presence of cyber threats, risks of unauthorized access to personal information, outdated IT infrastructure in certain institutions, and uneven levels of digital literacy among the population. The study emphasizes the need to strengthen information security measures and update the relevant legal and regulatory framework.

The work demonstrates that IT serves as a decisive catalyst for the modernization of public administration and its ability to respond to contemporary challenges. The successful transition of state operations to a digital format is crucial for the country’s competitiveness and its integration into the global digital landscape.

KEYWORDS: INFORMATION TECHNOLOGIES, PUBLIC ADMINISTRATION, DIGITAL TRANSFORMATION, E-GOVERNMENT, CYBERSECURITY, PUBLIC SERVICES, OPEN DATA, ARTIFICIAL

INTELLIGENCE, CLOUD TECHNOLOGIES, DIIA

ЗМІСТ

ВСТУП

Актуальність дослідження.

Світ нині переживає етап бурхливих змін завдяки інформаційним технологіям, які докорінно перебудовують усі сфери життя суспільства, особливо ж публічне урядування. Зростаюче впровадження комп'ютерних систем та автоматизація державних операцій змушують нас ретельно вивчати, яким чином ІТ впливають на результативність та надійність адміністративних дій.

В межах сфер публічного адміністрування, інформаційні технології відкривають широкі перспективи для вдосконалення робочих процесів, паралельно становлячись вирішальним елементом у забезпеченні цілісності даних та збереженні конфіденційної інформації. Безперервне накопичення цифрових відомостей та їхня масова обробка зумовлюють нагальну необхідність у посиленні захисту інформаційних платформ, що мають життєво важливе значення для державного апарату.

Сьогодні особливу вагу надають питанню гарантування інформаційної безпеки у державному секторі. Урядові структури, у розпорядженні яких перебуває надзвичайно делікатна й обмежена для доступу інформація, притягують увагу зловмисників та хакерських угруповань. Невпинне розширення масштабів кібернетичних атак та інцидентів із витоком даних констатує нагальну потребу ґрунтовнішого вивчення та створення дієвіших методів охорони інформаційних систем, що обслуговують публічні потреби.

Вивчення того, як інформаційні технології впливають на сферу державного управління, є ключовим аспектом для досягнення відкритості та підвищення дієвості урядування. Адекватне впровадження технологічних рішень дарує можливість значно покращити стандарти обслуговування населення, спростити адміністративні процеси та усунути зайві бюрократичні бар'єри. Таким чином, опрацювання цієї проблематики набуває надзвичайної важливості у сучасному контексті, адже суспільство очікує від публічного менеджменту більш

результативних та зрозумілих моделей функціонування.

забезпеченні безпеки інформаційного простору.

Мета дослідження - Завдання полягає у визначенні найбільш ефективних стратегій впровадження й використання цих технологій, спрямованих на забезпечення стабільного та продуктивного функціонування публічного сектору.

Завдання дослідження.

Для досягнення поставленої мети, необхідно вирішити наступні завдання:

1. Оцінити можливості, які надають нинішні інформаційні технології, для запровадження новаторських підходів у державному секторі.
2. Осмислити найсучасніші вектори розвитку та технічні новації у сфері державного адміністрування.
3. Провести аналіз систем електронного урядування, а також окреслити засадничі засади їхнього функціонування.
4. З'ясувати значення інформаційних систем управління для вдосконалення процедур державного управління.
5. Проаналізувати, яким чином інфовкрапте знання впливають на приватність персональної інформації у державній сфері.
6. Проаналізувати підходи до гарантування кіберзахисту в контексті застосування нинішніх інформаційних технологій.

Об’єкт та предмет дослідження.

Об’єктом дослідження є процеси впровадження та використання інформаційних технологій в сфері публічного адміністрування. Основною темою дослідження є інформаційні технології, застосовувані в публічному адмініструванні, та їхній вплив на забезпечення інформаційної безпеки.

Методологічна основа дослідження

Ґрунтується на використанні

комплексного підходу до аналізу впливу інформаційних технологій на публічне управління передбачає використання різноманітних методів дослідження. Зокрема, методи аналізу, синтезу та порівняльного аналізу сприяють глибокому вивченню.

Разом із цим, застосування експертних оцінок і моделювання відкриває можливості для прогнозування потенційних наслідків інтеграції новітніх технологій у систему державного управління.

Основою для дослідження є опрацювання науково-методичної літератури, що допомагає врахувати сучасні тенденції розвитку інформаційних технологій та оцінити їхній вплив на публічне управління. Важливим аспектом методологічної бази також стає аналіз практичних прикладів реалізації інформаційних технологій у сфері публічного адміністрування.

Наукова новизна дослідження.

Це дослідження відзначається науковою новизною завдяки цілісному підходу до аналізу впливу інформаційних технологій на систему публічного управління, а також їх взаємозв'язку з питаннями інформаційної безпеки. Основна інновація полягає у визначенні ключових чинників і принципів, які впливають на результативність використання інформаційних технологій у сфері публічного адміністрування. Окрім того, робота пропонує актуальні рекомендації щодо шляхів забезпечення інформаційної безпеки в умовах застосування сучасних ІТ-рішень.

Отримані результати та висновки можуть стати важливою основою для подальших наукових досліджень у галузі публічного управління та інформаційних технологій. Водночас вони мають практичну цінність для організацій і установ, які займаються інтеграцією новітніх технологій у діяльність публічної сфери.

Практичне значення.

Результати цього дослідження можуть бути використані у розробці та впровадженні стратегій ефективного використання інформаційних технологій в

сфері публічного управління. Крім того, рекомендації щодо забезпечення інформаційної безпеки можуть бути корисними для публічних установ та організацій у реалізації їхніх завдань та функцій.

*Структура та обсяг роботи***.** Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел (63 найменування).

1 ДОСЛІДЖЕННЯ АКТУАЛЬНИХ ІНФОРМАЦІЙНИХ ЗАСОБІВ У РАМКАХ ДЕРЖАВНОГО УПРАВЛІННЯ ТА ЇХНІЙ ВПЛИВ НА СОЦІАЛЬНЕ Й ЕКОНОМІЧНЕ ПРОГРЕСУВАННЯ СПІЛЬНОТИ

1.1. Можливості, що їх надають актуальні інформаційні технології, стосовно впровадження новаторських підходів у сфері публічних послуг.

Результати дослідження та сформульовані висновки можуть слугувати значущою основою для подальших наукових розвідок у сфері публічного управління та інформаційних технологій. При цьому вони також мають практичне значення для організацій і установ, які впроваджують сучасні технологічні рішення в процеси функціонування публічного сектору.

Одним із ключових аспектів є процес прийняття рішень і планування. Органи управління займаються розробкою стратегій та підходів до реалізації політик, спрямованих на розв'язання соціальних, економічних і інфраструктурних питань. Для ефективності цього процесу необхідні висока компетентність, аналітичне мислення та врахування інтересів різних категорій населення.

Іншим важливим аспектом є моніторинг і оцінка впровадження управлінських рішень. Відповідні служби здійснюють спостереження за ходом реформ, аналізують отримані результати та вносять необхідні корективи. Такий підхід допомагає звести до мінімуму можливі негативні наслідки й забезпечити максимальний позитивний ефект від ухвалених рішень.

Ключовим аспектом є гарантування відкритості та легкого доступу до інформації. Прозора діяльність органів влади виступає фундаментом демократичного суспільства. Громадяни мають право на отримання достовірної й вичерпної інформації щодо роботи державних установ.

До інших аспектів публічного управління можна віднести оптимізацію бюджетних видатків, реалізацію соціальних програм та підтримку ініціатив

громадських організацій.

Насамперед варто замислитися над питанням, чи є поняття публічного управління ідентичним до поняття публічної сфери. Ці терміни безумовно тісно пов’язані між собою, адже одне не може існувати без іншого. Водночас термін "публічна сфера" більш доречно вбачати як протилежність "приватної сфери". Якщо приватна або домашня сфера охоплює сімейне життя, особисті справи та стосунки з друзями, то публічна сфера є простором для висловлення думок, дискусій про колективні проблеми та суспільні інтереси. Термін "публічна сфера" здебільшого використовується у формі однини, проте в контексті складних диференційованих суспільств пізньої модерності, особливо в умовах глобалізації та впливу національних держав, слід сприймати публічну сферу як сукупність багатьох різних просторів. Саме тому доцільніше говорити про "публічні сфери" у формі множини, визнаючи існування безлічі варіантів фрагментації та конкуренції, як у фізичних публічних просторах, так і в онлайн-середовищі. У глобальному масштабі існує різноманіття публічних сфер, які коливаються від глибоко демократичних до авторитарних.

Вказані міркування одразу наголошують на важливості глобального погляду на публічні сфери і технічну допомогу. Починаючи дослідження, ми спершу зосереджуємося на аналізі взаємозв’язку в національному контексті, адже і технічна допомога, і академічне осмислення публічних сфер здебільшого розглядаються крізь призму національних процесів ухвалення політичних рішень, а також управління в державному та громадському секторі.

У цьому контексті інформаційні технології значно спростили та вдосконалили процеси, за допомогою яких уряди реалізовують свої функції та надають послуги населенню. Вони створили нові перспективи для підвищення ефективності, прозорості та відкритості в управлінні державними справами. Інформаційні технології розглядаються як фундамент та результат загального явища, відомого як інновації.

Інновації – це невід'ємний елемент сучасного суспільства, що визначає його

подальший розвиток та успішність. Інновації включають впровадження оригінальних ідей, сучасних технологій, нових продуктів і методів у різноманітних сферах життя. Це явище сприяє підвищенню конкурентоспроможності та забезпеченню стабільного розвитку суспільства в умовах глобалізації.

Економіка є однією з основних галузей, де інновації відіграють важливу роль. Використання новітніх технологій та сучасних методів виробництва дозволяє значно підвищити ефективність праці та покращити якість продукції. Завдяки цьому стимулюється економічне зростання і забезпечується покращення рівня життя громадян.

У галузі освіти та науки інновації мають значний вплив. Застосування сучасних підходів до навчання й досліджень сприяє покращенню якості освіти і підготовці висококваліфікованих фахівців. Прогрес у сучасних наукових і технологічних сферах відіграє важливу роль як один із основних чинників подальшого розвитку суспільства.

Ще однією важливою сферою залишається медична галузь. Інноваційні методи діагностики та лікування відкривають нові перспективи для збереження життя пацієнтів. Створення сучасних лікарських препаратів і розробка передових способів лікування допомагають вирішувати завдання, які донедавна здавалися нездоланними.

Окрім економіки та медицини, інновації відіграють важливу роль в інших аспектах нашого життя. Вони здатні змінити спосіб, у який ми працюємо з інформацією, отримуємо освіту, сприймаємо культуру, а також впливають на багато інших аспектів суспільного існування.

У цілому, інновації є ключовим елементом розвитку суспільства та держави, сприяючи вирішенню актуальних проблем та досягненню високих результатів у різних сферах. Завдяки інноваціям суспільство може досягати нових висот і вирішувати проблеми, які раніше здавалися непередбачуваними. Важливо постійно підтримувати інноваційну активність та створювати умови для

розвитку та впровадження новаторських рішень у всіх сферах життя [3].

Процеси цифровізації та впровадження сучасних ІТ можуть розвиватися на різних рівнях у вигляді таких інноваційних рішень:

- Смарт-міста та інфраструктура: За допомогою сенсорів, технологій Інтернету речей (IoT) та збору даних міста здатні ефективніше управляти енергоспоживанням, транспортом, водопостачанням і іншими ресурсами. Наприклад, системи "розумних світлофорів" можуть автоматично регулювати роботу світлофорів відповідно до інтенсивності руху транспорту.
- Електронне здоров'я: Запровадження електронних медичних карт і телемедицини сприяє поліпшенню доступу до медичних послуг та забезпечує ефективніший моніторинг стану пацієнтів [8].
- Електронне освітнє середовище: Розробка платформ дистанційного навчання, які враховують потреби різних категорій населення, відіграє важливу роль у розвитку освітнього процесу.
- Фінансові технології (FinTech): Сучасні інноваційні платіжні системи та електронні гроші відкривають нові можливості для швидкого й комфортного виконання фінансових операцій.
- Соціальні мережі та спільноти: Сучасні платформи для комунікації створюють ефективний і безпечний засіб взаємодії між органами влади та громадянами, сприяючи обміну актуальною інформацією.
- Електронна демократія: Електронні платформи для голосування та проведення громадських консультацій відкривають громадянам шлях до активної участі в управлінських процесах.

Ці нововведення здатні стимулювати зростання продуктивності у сфері державних послуг, піднести якість обслуговування населення та підприємницьких структур, а також удосконалити процес ухвалення керівних рішень.

Проте, разом із цим постають й проблеми, що стосуються приватності, кібербезпеки, а також етичних міркувань щодо застосування персональних даних .

Серед плюсів варто виділити:

- Підвищення ефективності та швидкості роботи: Впровадження інформаційних технологій уможливлює механізацію багатьох операцій, які донедавна потребували суттєвої затрати ресурсів та тривалого періоду. Як ілюстрацію, електронні інструменти для ведення реєстрів та обробки відомостей дають змогу оперативно стежити за низкою ключових параметрів.
- Підвищення доступності послуг: Цифрові майданчики дають змогу мешканцям здобувати потрібні відомості й сервіси через мережу, завдяки чому вони стають легшонабуваними для усяких прошарків суспільства та територій.
- Можливість здійснення аналізу та прогнозування: Інформаційно-технологічні аналітичні засоби дають змогу державним установам здійснювати глибший розбір різноманітних сторін соціокультурного поступу, що, своєю чергою, веде до ухвалення більш виважених керівних вердиктів.
- Посилення прозорості та відкритості: Онлайн-ресурси, призначені для публікації відомостей про ухвалені урядом рішення та здійснені кроки, дають змогу населенню краще орієнтуватися в ситуації та більш рішуче долучатися до формування політичного курсу.
- Зменшення витрат: Удосконалення робочих процесів та запровадження електронного документообігу здатне спричинити зниження адміністративних витрат.

Проте, важливо врахувати обмеження використання ІТ:

- Кібербезпека та конфіденційність даних: Створення систем для оберігання приватної інформації та убезпечення від злочинних дій у мережі набирає значущості.
- Доступність та ексклюзивність: Ключовим моментом є те, щоб

нікого не лишити осторонь, зокрема тих осіб, які не мають доступу до інформаційних технологій або ж бракує потрібних умінь для їхнього застосування.

Стійкість до змін та оновлень: Сучасні технології швидко змінюються, тому важливо мати механізми адаптації та оновлення ІТ-систем [4].\

Аналіз застосування інфо-комунікаційних технологій (ІКТ) у державному управлінні демонструє, що розгортання електронного урядування постає одним із головних засобів для досягнення продуктивності у сфері публічного Адміністрування. Застосування новітніх ІКТ дає змогу вносити суттєві корективи у роботу владних структур, зокрема, впроваджувати докорінно інші моделі функціонування цих інституцій.

Ключова перевага, яку надають інформаційно-комунікаційні технології (ІКТ), полягає у розширенні доступу до різноманітних послуг та суттєвому скороченні тягаря бюрократичних формальностей. Як приклад, запровадження електронного волевиявлення здатне радикально спростити організацію та проведення виборчих процесів, що є особливо актуальним у нинішніх складних військово-політичних реаліях України. Крім того, завдяки використанню онлайн-платформ для консультацій та плебісцитів, громада отримує реальні важелі для підвищення своєї активності та глибшої інтеграції у механізми прийняття рішень .

Інформаційно-комунікаційні технології спроможні стати в нагоді й у сфері державного адміністрування, а саме за умов:

- Забезпечують широкий доступ до інформації.
- Дозволяють зберегти час та кошти.
- Забезпечують широкий доступ до послуг.
- Дозволяють забезпечити безпеку даних.

Проте, запровадження електронних урядових систем наштовхується на низку викликів, до яких належать обмежена доступність мережі Інтернет, нестатнє фінансування заходів з інформатизації, а також зарегульованість та повільність у роботі чиновників. Характерною рисою застосування новітніх

інформаційно-комунікаційних технологій у державному адмініструванні є ситуація, коли паперовий та електронний документообіг співіснують, а перехід до виключно електронного формату відбувається неспішно. Соціальні мережі

постають як багатообіцяючий засіб комунікації між державними структурами та громадянами, що розкриває значний потенціал для органів публічної влади.

Наведений науковий пошук також свідчить про те, що поточний етап формування інформаційного соціуму та сфери інформаційно-комунікаційних технологій (ІКТ) в українських реаліях, коли зіставляти його зі світовими орієнтирами, є недостатнім і не сягає стратегічних завдань розвитку нашої держави. Наразі у механізмах державного управління України відчувається гостра необхідність у впровадженні інноваційних засобів, підходів та технічних рішень, що мають на меті збільшення його дієвості.

Стосовно питань, пов'язаних із соціальною сферою, демографією та політикою, варто звернути увагу на запроваджені інформаційно-технологічні заходи, спрямовані на протидію глобальній пандемії COVID-19. Цей випадок охоплює як уже втілені новаторські рішення, так і ті ідеї, що залишилися на стадії пропозицій, хоча й цілком можуть бути обґрунтованими.

Спалах COVID-19 завдав колосального удару по галузях, як-от охорона здоров'я, бізнес, освіта та загальна економічна сфера. Аби громада змогла стримати розповсюдження коронавірусу, на перший план вийшли такі інструменти, як телемедицина, віддалене виконання обов'язків та навчання через інтернет. Епідемія слугувала поштовхом, що спричинив шалений зріст потреби у застосуванні передових розробок задля мінімізації негативних наслідків поширення COVID-19 на наше буття. Такий стан речей не просто розкрив двері для впровадження технічних інновацій, а й створив унікальний шанс для глибинного аналізу наукових здобутків та практичного втілення технологій, зокрема у сферах опрацювання даних, організації робочих процесів, а також проєктування й експлуатації технічних засобів.

Стрімкий зсув до телемедичних послуг, віддаленої залученості до праці та

навчання через інтернет, спричинений викликом коронавірусу, слугує вагомим аргументом на користь того, що цифрові засоби пропонують низку суттєвих плюсів та здатні бути ключовими у справлянні з ризиками, які постали через карантинні обмеження в період пандемії й надалі. Загальновизнаним є той факт, що інформаційні системи та інформаційні технології (ІС/ІТ) демонструють значну вагу у сфері охорони здоров'я, допомозі у формуванні клінічних рішень.

Численні ІТ-професіонали вдавалися до різноманітних кроків, аби підсобити у протистоянні пандемії. Сюди входила розробка засобів для боротьби з вірусом, моніторинг та передбачення його розповсюдження, а також забезпечення кібербезпеки лікарень. Науковці, які працюють у галузі інформаційних систем та технологій, долучилися до загальносвітових заходів із подолання COVID-19 та інших епідемічних загроз, спираючись на свій накопичений досвід у кризовому реагуванні, процесах прийняття рішень, дистанційній зайнятості, керуванні віртуальними колективами, роботі з масивами даних та інших суміжних сферах.

Наразі бракує значного обсягу наукових розробок з інформаційних систем, спрямованих на протидію COVID-19 чи іншим глобальним кризам у сфері охорони здоров'я. Хоча небезпека коронавірусу дещо зменшилася, провідні вчені, інженерний корпус, медичні фахівці та ІТ-експерти не припиняють свою діяльність у цій галузі, прагнучи вийти на ще більш суттєві здобутки.

У світі, якщо подивитися на те, як розвивається освіта, беручи до уваги можливості, які дають новітні інформаційні засоби, то стає очевидним, що запровадження чогось нового (інновацій) у сфері державних послуг є надзвичайно важливим. Документ від ЮНЕСКО, який аналізує "Порядок сталого розвитку після 2015 року", чітко вказує: у цей новий час інформації університетська освіта має перетворитися на головну рушійну силу поступу. При цьому, будь-які нововведення у різних частинах життя суспільства мусять характеризуватися великою швидкістю змін та здатністю оперативно пристосовувати знання, особливо коли йдеться про ІТ [14]. З огляду на

вищесказане, роль держави стає значно вагомішою, адже вона зобов'язана гарантувати, що кожен має доступ до освіти високої якості, володіє глибокими знаннями, а також може здобути необхідні уміння та професійні якості. Сучасне буття, у якому обертається людина, набирає рис заплутаності та розбіжностей.

Щоб вибудувати доцільну життєву парадигму, потрібен доволі значний інтелектуальний та креативний хист, непересічна майстерність. З огляду на це, однією з найважливіших функцій освітніх закладів вищого рівня є стимулювання особистісного і фахового становлення тих, хто навчається. Цей розвиток мусить мати виразний прогресивний вектор, а процес осягнення нового матеріалу зобов'язаний інтегрувати впровадження передових методик.

У сучасному світі термін "Soft skills", що прийшов із закордону, набирає обертів. Він охоплює наші особистісні риси та вміння. На відміну від професійних чи технічних здібностей, це не лише те, що ми знаємо, а й те, як ми поводимося у різних обставинах. До "м'яких навичок" можна зарахувати будь-яку здібність, яку можна схарактеризувати як індивідуальну рису або усталений спосіб дії [15]. Навички взаємодії з іншими людьми та здатності до комунікації є більш вузькими підгрупами таких "софт-скіллів", які роботодавці часто цінують у претендентах на вакансії. Ось кілька з найбільш затребуваних софт-скіллів:

- Ефективні комунікаційні навички.
- Командна праця.
- Надійність.
- Адаптованість.
- Управління конфліктами.
- Гнучкість.
- Лідерство.
- Вирішення проблем.
- Відкритість новому.

Досить великий спектр зазначених умінь та навичок набувається в результаті впливу суспільства і розвивається на різних етапах людського життя (дошкільна освіта, загальна середня освіта, ВНЗ). Сфера огляду освіти та наукового поступу, що слугують рушійними силами для розвитку публічного простору, мусить, у контексті втілення новітніх методик, брати до уваги значущість "м'яких умінь" і мати в своєму арсеналі відповідні соціологічні та психологічні моделювання, націлені на культивацію означених компетенцій серед різнорідних груп громадян .

Коли ми розмірковуємо про педагогічну діяльність, варто підкреслити потребу у формуванні інструментарію, який був би водночас доволі простим у застосуванні, але й максимально гнучким для забезпечення індивідуально-фахового зростання тих, хто навчається. Завдання такого інструменту — оголити сутність та перебіг цього зростання у контексті застосування новаторських освітніх підходів та архітектури навчального простору. У зв’язку з цим, на часі є ревізія ключових складових освітнього процесу: навчального матеріалу, способів організації, прийомів роботи, технічних засобів, дидактичного супроводу (включно з навчальними посібниками) та ролі викладача.

Концепція "педагогічні технології" зазнала трансформації, давши початок сучаснішим термінам: "освітні технології", "педагогічні технології" та "технології навчання". Освітні технології, своєю чергою, відображають ширшу парадигму розвитку освітньої сфери, формуючи цілісний освітній континуум. Вони слугують інструментом для футурологічного бачення розвитку освіти, дають змогу точно проєктувати та планувати діяльність, передбачати очікувані результати, а також чітко окреслювати відповідні стандарти та навчальні цілі. Серед ілюстрацій освітніх технологій можна назвати доктрини освіти та існуючі освітні системи.

Коли йдеться про освітні технології, вони, по суті, відображають загальноосвітню стратегію. Натомість педагогічні ж підходи спрямовані на втілення цієї стратегії у життя, а саме — на тактичні кроки її імплементації в

освітній континуум, що досягається через запровадження відповідних моделей та ідентичних їм управлінських структур, які керують цим процесом.

Ми оглянули лише обмежений набір запроваджених процедур, у яких навіть найдрібніша частка стратегічного потенціалу інноваційної свіжості відсутня.. Неможливо недооцінити користь Інтернету як простору публічності.

Розмова про те, чи може Інтернет сприяти демократії, не повинна обмежуватися лише перерахуванням його переваг чи вроджених якостей, на кшталт оперативності, охоплення чи його власне "вільного" устрою. Те саме стосується й його недоліків чи побічних явищ, як-от фрагментованість чи анонімність. Сукупність цих аспектів не дає права бачити в Мережі лише чергову версію традиційних ЗМІ та національного громадського простору. Його комунікація, що відбувається через комп'ютери, започатковує інший тип публічної сфери — "розподілений", а не централізований, із новими способами взаємодії.

Під "розпорошеним" ми уявляємо собі, що комп'ютерні технології, зокрема Мережа, роблять публічний простір "розфокусованим"; це радше сукупність окремих громад, аніж єдиний, чітко окреслений та всеосяжний публічний майданчик, де всі учасники комунікації можуть зустрітися. Замість того, щоб потрапити у вже сформований публічний простір, Інтернет набуває статусу публічної сфери виключно завдяки діям тих, хто бере активну участь у роздумах та демократичних процесах.

З розвитком Інтернету як суспільної сфери можна очікувати його «реінтермедіалізацію». Це означає появу нових посередників, які протистоять його приватизації та індивідуалізації, спричиненим постачальниками доступу та контенту для комерційних цілей, і які створюють користувача як учасника публічної сфери.

Є кілька причин вважати, що існуючі демократичні інститути недостатньо

справляються з цим завданням. Уряди заохочують перехід різних медійних платформ, що слугують для спілкування, у приватні руки. Це стосується не лише мережі Інтернет, а й ефірного часу. Навіть якщо Інтернет за своєю природою не є антиавторитарним, і навіть якщо владні структури були б схильні більше дбати про збереження загальнодоступності цифрового середовища, досі залишається невирішеним, чи здатна ця форма обміну інформацією існувати поза межами того, як державна влада упорядковує просторово-часові рамки, включно з публічним часом та місцем для дебатів.

Отже, нинішні інформаційні засоби надають необмежений простір для запровадження свіжих підходів у царині державного керівництва. Зокрема, їхня здатність має першорядне значення для дієвості та прозорості функціонування владних і виконавчих інституцій. Конкретні плюси застосування інформаційних інструментів включають спроможність вдосконалити процес ухвалення рішень через аналіз чималих масивів інформації. Це уможливлює приймати більш виважені та обґрунтовані висновки, котрі адекватно відображають справжні потреби соціуму. Ба більше, запровадження електронних майданчиків та сервісів суттєво полегшує комунікацію громадян із державними установами. Це робить надання послуг більш досяжним та комфортним для мешканців. Прогрес сучасних інформаційних засобів також підштовхує до новаторства у сфері публічного адміністрування. Необхідне безперервне вдосконалення й розширення технологій, що стимулює генеровацію передових рішень та розробок задля оптимізації управління державою. Залучаючи ІТ, можна формувати відкриті ресурси для оприлюднення відомостей про роботу урядових органів, що сприятиме прозорості та вільному доступу громадськості до суттєвих даних.

Інформаційні технології надають можливість раціонально розподіляти та використовувати ресурси, що є особливо важливим у ситуаціях фінансової обмеженості.

1.2. Сучасні напрями та технологічні новаторства у сфері державного адміністрування.

Державне адміністрування складає невід'ємну частину нинішнього укладу суспільства. Його функція та вага зумовлюються наявністю дієвого апарату засобів, націлених на опанування суспільно-економічних потреб та сприяння збалансованому прогресу держави. У цьому фрагменті будуть проаналізовані базові уявлення та постулати, що формують підвалини державного управління, його структурні компоненти та кінцеву мету.

Перш за все, слід зосередитись на ключовому осмисленні сутності державного урядування. Згідно з нинішнім розумінням, державне урядування являє собою набір структурних та операційних кроків, покликаних втілювати на практиці стратегічні вектори та місії, поставлені перед соціумом. Воно охоплює без винятку всі складові державного втручання у процеси, що стосуються економіки, суспільства та політичної сфери.

Аби публічне управління працювало як слід, мусить бути дотримано низку ключових засад. Не останньою за значенням є принцип чинності норм та легітимності рішень. Це означає, що керівні структури зобов'язані керуватися встановленими правовими актами та мати належне суспільне схвалення (мандат) для своєї діяльності.

Наступною ж важливою засадою виступає яскравість і недвозначність. Вони означають, що відомості про ухвалені рішення та кроки уряду мають бути у вільному доступі для люду. Ця засада є рушійною силою для демократичної суті керування та дає змогу громадянам формувати вплив на визначальні кроки.

Ще одним важливим принципом є ефективність та результативність. Публічне управління повинно бути спрямоване на досягнення конкретних цілей

та покращення якості життя громадян. Важливо визначати чіткі критерії успіху та вчасно аналізувати результати.

У межах державного управління виокремлюють низку визначальних елементів. Насамперед, це державні виконавчі структури, які відповідальні за впровадження у життя ухвалених постанов та планів. Серед їхніх функцій – нагляд за дотриманням чинного законодавства та встановлених норм.

Друга частина – це законодавчі органи, котрі встановлюють засадничі засади роботи системи та ухвалюють нормативні акти. Цей рівень є головним представницьким органом народу у владних інституціях.

Наступним суттєвим елементом виступає залучення неурядових організацій та різноманітних ініціатив громадян, котрі здатні чинити тиск на процес ухвалення рішень завдяки своєму активному включенню у публічні обговорення.

Основне завдання державного адміністрування полягає у підтриманні сталості та прогресу соціального устрою. Сфера його відповідальності охоплює не лише заперечення порушення законних прав та вольностей населення, а й формування позитивного середовища для економічного піднесення та втілення принципів соціальної рівності.

Коли Україна проходила етап трансформацій на зорі дев'яностих, концепція "державного управління" набула статусу свідомого, структурованого втручання влади у розвиток суспільства. Цей процес охоплює не лише функції, що виконуються урядовими інституціями та особовим складом адміністрації, але й діяльність різноманітних інституційних утворень, які зосереджені на формуванні та регулюванні матеріальних благ, а також соціальної та духовної сфери.

У сучасних умовах важливо розглядати цей процес як невід'ємний компонент становлення та розвитку суспільства, адже саме від ефективності публічного управління залежить вирішення багатьох суспільних проблем.

Підсилення інформаційного аспекту – це один із головних напрямків еволюції державного адміністрування. Завдяки новітнім технологічним розробкам та полегшенню доступу до відомостей, відкриваються шляхи для більш дієвого впливу на формування управлінських вердиктів, беручи до уваги запити різноманітних верств населення та окремих громадян. Урядовці тепер спроможні швидко обробляти відомості та відповідно реагувати на суспільні зрушення.

Ще однією помітною течією виступає посилення відкритості та зрозумілості того, як здійснюється управління. Суспільство має законне право бути обізнаним щодо того, що роблять владні структури, і повинно мати змогу впливати на формування ключових рішень. Взаємодія між громадянами та державними установами на всіх етапах управлінської роботи є невід’ємною складовою нинішньої моделі публічного адміністрування.

Окрім вищесказаного, необхідно підкреслити посилення ваги органів місцевого самоврядування в структурі управління публічними справами. Згідно з основним законом України, якраз місцеві ради володіють повноваженнями щодо здійснення місцевого самоврядування і відповідають за розв'язання питань, що стосуються локальних потреб. Їхня функція у процесі забезпечення громадян належним рівнем сервісу та реагування на їхні запити набуває вирішального значення. Також спостерігається тенденція до підвищення важливості стратегічного бачення в межах публічного адміністрування. Створення та реалізація планів стратегічного розвитку сприяє більш злагодженій взаємодії між різними інституціями влади, спрямовуючи їх зусилля на спільні суспільні цілі.

Враховуючи вищезазначені тенденції, слід підкреслити, що сучасне публічне управління є динамічним та постійно змінюється під впливом різних факторів.

У межах такого підходу, керування інноваціями набуває статусу вирішального елемента, завдяки якому можливо упорядковувати та успішно запроваджувати передові задуми, технічні рішення та підходи у кожен аспект функціонування підприємства. Хоча сутність самого поняття "інновація" ми вже розкрили далі, то як же тоді слід розуміти термін "управління інноваціями"?

Сучасне керівництво, сфокусоване на новаторстві, являє собою багатогранний механізм управління, головною метою якого є формування середовища, що заохочує появу та дієве застосування інноваційних рішень у кожному аспекті функціонування установи. Щоб досягти повного розуміння стратегічного підходу до керівництва, варто зосередитись на ключових засадах, на яких він ґрунтується.

1. Стратегічна перспектива. Першим наріжним каменем управління інноваціями є формування зрозумілої та сміливої стратегії. Ця стратегія зобов'язана окреслити призначення та вектори спрямування інноваційної діяльності, беручи до уваги чинники як у межах компанії, так і поза нею. Критично необхідно встановити вимірні цілі, завдання та прогнозовані здобутки, а також прописати маршрути для досягнення цих установок. Подібно до навігаційного приладу, стратегія виступає як путівник для всієї структури у ході еволюційного інноваційного поступу.

2. Керівна роль та забезпечення підтримки згори. Згідно з цим принципом, вищий менеджмент організації несе пряму відповідальність за динамічне заохочення та забезпечення сприятливих умов для будь-яких інноваційних починань. Керівні особи зобов'язані демонструвати прихильність до нових ідей, брати на себе проактивну роль у їхньому втіленні, слугуючи взірцем для решти персоналу. Їхня недвозначна залученість та щире прагнення до інновацій слугують потужним стимулюючим повідомленням для усієї структури.

3. Втягнення колективу. Сучасний підхід до керівництва наголошує на потребі долучати абсолютно усіх співробітників до процесу розробки та

реалізації будь-яких новацій. Необхідно налагодити системи для фіксації та оцінки пропозицій, що надходять від команди, забезпечити їм шанс долучатися до інноваційних ініціатив та відзначати їхні зусилля у цьому напрямку.

4. Комплексний підхід. Управління інноваціями має бути інтегровано у всю структуру керівництва підприємства. Це означає, що інноваційні процеси необхідно впроваджувати у кожну складову роботи фірми – операційну діяльність, просування продукції, фінансову політику, управління персоналом та інші сфери. Слід ретельно аналізувати наслідки впровадження новацій як для внутрішнього функціонування, так і для зовнішніх бізнес-операцій, задля чого всі ресурси мають бути мобілізовані на досягнення єдиного визначеного результату.

5. Культура інновацій. Формування ґрунту, що сприяє впровадженню нового – це вирішальна складова успішної адміністративної діяльності. Йдеться про формування атмосфери, де панують відкритість, заохочення та належна оцінка оригінальних задумів. Необхідно мотивувати персонал до розробки проривних концепцій та забезпечувати ресурси для їхнього втілення [28] .

6. Співпраця. Ефективне управління інноваціями передбачає налагодження зв'язків із різноманітними суб'єктами: іншими фірмами, науковими осередками та новоствореними підприємствами. Завдяки цьому забезпечується взаємообмін досвідом та технологічними наробками, що, у свою чергу, стимулює швидке та результативне впровадження новацій.

7. Параметризація та нагляд. Нагляд за досягненнями та визначення значущості інноваційних ініціатив становлять невід'ємний елемент їхньої життєздатності. Регулярний розбір дієвості дає змогу ідентифікувати перешкоди й запроваджувати потрібні зміни. Необхідно брати до уваги як вимірювані, так і суб'єктивні критерії успішності, а також коригувати курс дій відповідно до здобутих висновків.

Покладені в основу, ці засади формують фундамент для дієвого керівництва інноваціями всередині установи.

Державне керування виступає визначальним елементом прогресу соціуму у всіх державах. В нинішніх обставинах спостерігається швидке вдосконалення технічних засобів, що значно відбивається на концепціях та інструментах го судженнями суспільними явищами. Технічні новинки у сфері державного адміністрування набувають дедалі більшої ваги для гарантування дієвого та успішного функціонування нинішніх управлінських структур.

Сучасні технологічні прориви в царині державного адміністрування включають інтеграцію найновіших інформаційних систем, обробку даних у режимі, близькому до миттєвого, залучення елементів штучного інтелекту, а також формування цифрових майданчиків задля оптимізації надання послуг населенню. Основні засади, якими керуються ці технологічні новації в системі публічного врядування:

1. Цифрова трансформація – один із ключових принципів. Своєю чергою, це тягне за собою зміну парадигми: від застосування звичних бюрократичних регламентів до впровадження передових інформаційних рішень задля підвищення ефективності функціонування органів влади.

2. Відкриті дані. Надання змоги користуватися загальнодоступними даними становить іще один ключовий засадничий принцип. Подібна практика веде до посилення прозорості та відкритості, якими мають керуватися у своїй роботі державні органи у взаєминах із соціумом.

3. Електронне урядування. Запровадження в дію електронного урядування уможливлює надання адміністративних послуг у цифровому форматі, спрощуючи таким чином контакт та комунікацію поміж державою та її громадами.

4. Інноваційний лідер. Ключовою є наявність певної особи, котра б несла відповідальність за інтеграцію технічних новацій у діловодство. Лідер інноваційного спрямування допомагає узгоджувати та впроваджувати зміни та новинки.

Нововведення у державному урядуванні здатні слугувати вагомим засобом для досягнення дієвості та результативності у розпорядженні державними справами. Україна не лишається осторонь цього процесу, і ми бачимо чимало зразків вдалого впровадження інновацій у сфері публічного адміністрування на теренах нашої держави.

Приміром, український відкритий бюджет слугує одним із найвдаліших зразків застосування новаторських підходів у державному управлінні на території України. Ще одним показовим моментом є запуск електронного урядування в Україні, завдяки чому вдалося знизити рівень корупції та поліпшити дієвість керівництва державними процесами. Ба більше, в Україні запровадили новітні техніки управління муніципальними фінансами, зокрема електронні платформи для нарахування податків і формування бюджету, що сприяло підвищенню раціональності розпорядження місцевими коштами.

Давайте тепер сфокусуємося на першому державному проєкті, якому матимемо честь приділити пильну увагу, а саме – програмному рішенню під назвою "Прозоро". Дана система "Прозоро" являє собою електронний майданчик для проведення державних закупівель на території України, розроблений з ключовою метою – гарантувати відкритість та результативність у процесі державних закупівель. Завдяки "Прозоро", уповноважені державні й комунальні структури мають можливість публічно оголошувати конкурси стосовно придбання продукції, виконання робіт чи надання послуг, тоді як суб'єкти господарювання змагаються між собою у цих торгах за право здійснити відповідні поставки для потреб держави. Будь-яка дія, що відбувається під час торгів, є доступною для огляду будь-якій зацікавленій особі через спеціально створений інтернет-ресурс. Фактично, ця розробка вважається одним із найбільш видатних і вдалих зразків впровадження інноваційних підходів у сферу державного управління у межах нашої країни.

Зокрема, у царині державних інновацій варто звернути увагу на закордонний досвід, як от ініціатива “Smart Dubai”. Цей проєкт, розпочатий у

2014 році, мав на меті перетворити Дубай на справді “розумне” місто. В основі програми лежить впровадження передових технологій, таких як блокчейн, штучний інтелект та аналіз великих масивів даних, що спрямовано на підвищення рівня життя як для резидентів, так і для гостей міста. У рамках “Smart Dubai” реалізуються різноманітні заходи, приміром, “DubaiNow”, “DubaiPay” чи “DubaiID”, які надають можливість усім – громадянам та діловим колам – користуватися спектром державних сервісів у режимі онлайн. Окрім того, програма охоплює кроки з удосконалення міської інфраструктури транспорту, підвищення енергоощадності та покращення екологічної ситуації.

Програмне забезпечення "Smart Dubai" інтегровано до загальної концепції "Dubai Plan 2021". Ця ініціатива спрямована на те, щоб перетворити Дубай на одне з найрадикальніших у плані інновацій та найприємніших для життя міст на планеті. Завдяки "Smart Dubai" місто стає значно простішим у користуванні як для тих, хто тут мешкає, так і для гостей, паралельно усуваючи необхідність у великій кількості документів та, як наслідок, заощаджуючи час і фінансові ресурси.

Розглядаючи світовий досвід, неможливо оминути Естонію та її здобутки у сфері електронного урядування. Естонська система е-урядування визнана однією з найвдаліших на планеті. Впроваджена в 2001 році, вона стала прикладом для наслідування для багатьох країн [36]. Основні компоненти системи Estonian e-Government включають:

- X-Road являє собою децентралізовану інформаційну екосистему, що уможливлює інтерактивний обмін даними між різноманітними системами. Як приклад, правоохоронні органи отримують спрощений доступ до відомостей із медичних реєстрів, податкових баз чи корпоративних даних, і така ж двосторонність взаємодії забезпечена й для інших установ. Впровадження X-Road спричинило помітне поглиблення взаємодії між державними установами та суттєве скорочення обсягів документації, що звільняє службовців від рутинної паперової роботи задля сфокусування на критично важливих, людино-орієнтованих процесах.

- Естонські державні послуги в цифровій формі: Левова частка державних сервісів у країні вже переміщена у мережу. Це дає змогу як звичайним громадянам, так і суб'єктам господарювання отримувати потрібні послуги оперативно та без зайвих клопотів, включно з оформленням реєстрації місця проживання, поданням запитів на видачу чи обмін паспорта чи посвідчення водія, а також здійсненням реєстрації юридичних осіб у режимі онлайн.

- Електронні свідоцтва особистості: Естонія володіє найдосконалішою у світі державною системою посвідчень особи. Ці картки не лише забезпечують мешканцям доступ до усіх захищених електронних сервісів у межах держави, але й дають змогу громадянам накладати свій підпис на документи та брати участь у голосуванні дистанційно.

Завдяки цим складовим, як звичайні люди, так і бізнес-суб'єкти спроможні ефективно та із зручністю здобувати державні сервіси. Це також сприяє скороченню обсягів документації, звільняючи державних працівників для виконання справ, які вимагають їхньої особистої участі, замість монотонних, повторюваних операцій.

Якщо говорити про наші вітчизняні досягнення, то варто зосередити пильну увагу на одному з найбільш вдалих починань, що стосується впровадження новітніх рішень в царині інформаційних технологій у межах державного сектору.

"Дія" (скорочення від "Держава і ти", англійською Diia) — це електронний застосунок для смартфонів, а також відповідний веб-ресурс. Він належить до складових програми цифровізації України та був створений зусиллями Міністерства цифрової трансформації нашої держави. Ця ініціатива була вперше анонсована у 2019 році, а повноцінний запуск відбувся вже наступного, 2020 року.

Електронні посвідчення водія, як внутрішні, так і закордонні паспорти, а також низку інших документів, стало можливо зберігати завдяки використанню цього застосунку. Зберігаючи їх у цифровій формі, користувачі отримують

змогу надсилати їхні копії, скажімо, при потребі скористатися банківськими чи поштовими сервісами, під час поселення у готельних закладах чи в низці інших обставин.

Більше того, застосунок "Дія" (його мобільна версія чи веб-версія) надає доступ до низки важливих державних сервісів. Серед них сервіс "єМалятко", який об'єднує послуги, пов'язані з народженням дитини, реєстрація підприємницької діяльності та ФОП у режимі онлайн, можливість сплатити податкові зобов'язання та подати відповідні декларації, отримання електронного підпису, придатного для засвідчення будь-яких документів, а також зміна зареєстрованого місця проживання та чимало іншого.

Мається намір стратегічного характеру, що передбачає повсюдну інтеграцію усіх державних послуг у платформу "Дія" із забезпеченням їхньої доступності до настання 2024 року.

Станом на листопад 2023 року число користувачів цієї платформи перевищує сімнадцять мільйонів осіб. На веб-ресурсі можна скористатися понад сімома десятками послуг, тоді як у мобільному застосунку налічується дев'ять послуг і п'ятнадцять електронних документів. Додатково, на офіційному сайті "Дія" заявлено про наміри запровадити ще понад дев'яносто проектів.

На рівні муніципалітету варто також відзначити програму безпеки руху, що діє в Одесі. Це цільова програма міста, мета якої — зменшення числа ДТП, покращення стану дорожньої інфраструктури та підвищення рівня захищеності осіб, залучених до дорожнього руху.

Програма була затверджена Одеською міською радою у 2019 році [38].

Основними завданнями Програми є:

1. Розробка плану стабільної міської мобільності.

2. Реалізація домовленостей у межах підписаних угод з Європейським

інвестиційним банком.

3. Впровадження всеосяжної цифрової транспортної схеми міста. Освоєння передових інформаційних технологій для формування бачення та передбачення розвитку міської транспортної мережі. Застосування моделювання та передбачення з метою ухвалення обміркованих, фінансово виправданих рішень.

4. Впровадження апаратно-програмних комплексів, призначені для детального моделювання функціонування світлофорних систем, міських розв'язок та інших складових транспортної мережі населеного пункту.

5. Початок облаштування безпечної інфраструктури міста.

6. Перехід на дорожню розмітку із пластику.

Проте, у фокусі нашого вивчення лежить таке управлінське рішення, яке б забезпечило найкращу ефективність у контексті державного управління, а саме – спосіб інтеграції міських систем із сервісом «Штрафи UA».

«Штрафи UA» являє собою загальнодержавну платформу, що дає змогу громадянам оперативно з'ясувати, чи мають вони несплачені штрафи (отримані від патрульної поліції, завдяки відеофіксації або за порушення правил паркування у низці муніципалітетів) та здійснити їхнє миттєве і безпроблемне погашення.

Аби людям було простіше, доступні для користування веб-ресурс, мобільний додаток на платформі Android, чи бот у Telegram, які дозволяють з'ясувати наявність штрафів, використовуючи номерний знак транспортного засобу або водійське посвідчення. Згідно з даними, оприлюдненими Одеською міською радою, протягом менш як семи днів виявляється понад дві тисячі випадків порушення правил паркування, що забезпечує надходження до місцевого та державного скарбів суми, наближеної до одного мільйона гривень.

У нинішній ері стрімких трансформацій та суспільних викликів, наявність динамічних змін зобов'язує апарати публічного адміністрування невпинно проводити оцінку та приводити свою діяльність у відповідність до новітніх

обставин.

Новітні тенденції та технологічні інновації відіграють ключову роль у цьому процесі. Однією з основних тенденцій є перехід до цифрового управління. Використання сучасних інформаційних технологій та електронних платформ дозволяє оптимізувати процеси взаємодії між органами влади та громадськістю, а також забезпечує швидкість та доступність інформації.

Ще однією значущою тенденцією постає зростання ваги громадськості у фарватері формування та втілення рішень. Коли громадські формування та небайдужі громадяни залучаються до розмови з державними структурами, це веде до більш успішного врегулювання питань та справжнього врахування потреб соціуму.

Окрім того, слід звернути увагу на помітну тенденцію до поглиблення транскордонної співпраці у царині державного адміністрування. Обмін напрацюваннями та імплементація випробуваних методів із закордонних держав дає змогу не допустити повторних хиб та досягнути вагоміших результатів у процесах управління.

Набуття все більшої ваги прозорістю, відкритістю та підзвітністю утверджується як наріжний камінь нинішньої системи державного адміністрування. Суспільство має завищені сподівання щодо того, щоб урядові кроки у прийнятті рішень були розкриті, а звітність про їхнє виконання була загальнодоступною. Усі ці нововведення та вектори розвитку у сфері державного керування націлені на підвищення добробуту населення, сприяння сталості та прогресу соціуму. Ключовим моментом для досягнення цих завдань є акцентування уваги на впровадженні передових технологічних рішень та активному залученні громадян до процесів управління.

Висновки за розділом 1

1. Розділ 1 присвячений ретельному аналізу сучасних інформаційних технологій та їхнього впливу на публічне управління з метою сприяння

для забезпечення чесного суспільного та фінансового поступу нації. Проведений аналіз найголовніших моментів окреслює значущі вектори для майбутніх здвигів та застосування новеньких рішень.

Дослідження виявило, що цифрові засоби перетворюються на основний важіль для імплементації інновацій у сфері державного керування. Вони не просто налагоджують буденні процедури, а й формують підґрунтя для оперативного та результативного розв'язання питань, пов'язаних із життям і господарством. Можливості технологій криються у їхній спроможності гарантувати високу точність, відкритість та миттєвість під час ухвалення та реалізації керівних указів.

2. Привертається увага до актуальних тенденцій та інновацій в галузі публічного управління. Використання цифрових платформ, електронних сервісів та засобів комунікації з громадськістю стає необхідною складовою для створення відкритого та демократичного середовища. Технології дозволяють громадянам брати активну участь у процесах управління та забезпечують шляхи для реалізації їхніх поглядів та ініціатив.

Розділ 1 надає глибокий огляд інформаційних технологій у контексті публічного управління, виокремлюючи їхню ключову роль у сприянні справедливому соціальному та економічному розвитку. Акцент на потенціалі технологій та їхній ролі у створенні відкритого та гнучкого управлінського середовища підкреслює важливість поєднання інновацій та публічного управління для досягнення сталого прогресу суспільства.

2 ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ЗАСОБІВ У ГРОМАДСЬКОМУ УПРАВЛІННІ

2.1 Електронні урядові системи: становлення, структура та здібності.

Набуваючи чинності у світлі стрімкого поступу цифровізації, інтеграція електронних урядових рішень (ЕУР) стала незаперечною вимогою сьогоденного формату державного управління. Відтепер ці системи окреслюють новий вектор для регламентації, де використання технологічних інструментів має на меті оптимізацію процесів та стимулювання ефективного діалогу між державними інституціями і громадянами. Однак, перед тим, як заглибитися у сутність та функціонал ЄУС, спершу варто сфокусуватися на чинниках, що зумовили їхнє постання, а також провести детальний огляд основних елементів їхньої конструкції та структури. Нашим завданням є простежити етапи розвитку, фундаментальні принципи роботи, а також чисельні можливості, які пропонують сучасні цифрові уряди. Ба більше, ми обов'язково розглянемо перешкоди, які гальмують розвиток цих систем, і потенційні шляхи їхнього подальшого вдосконалення з огляду на швидкий технологічний прогрес.

Електронне урядування, хоча й є доволі новою ідеєю, має вже тривалий шлях становлення. Задля чіткості в розумінні, ми окреслили два основні етапи у світовій еволюції систем електронного врядування.

Фаза первинного становлення електронного урядування. Витоки електронного урядування (e-government) простежуються аж до 60-х та 70-х років минулого століття, коли комп'ютерні системи уперше стали залучатися до обробки даних у межах адміністративних процесів.

Спроби впровадити механізацію та цифрові системи в низці держав мали певні обмеження, проте саме цей час ознаменував перші етапи переходу державних установ на електронний формат роботи.

Друга фаза подій розпочалася із приходом Інтернет-буму та

утвердженням поняття "електронного уряду". Протягом дев'яностих і двохтисячних років, коли Інтернет-сфера почала стрімко розвиватися, відкрився новий шлях для переведення державного управління у цифровий формат. Уряди різних країн, як-от Сполучені Штати, Велика Британія, Сінгапур та Швеція, активно займалися розробкою та інтеграцією цифрових сервісів, аби спростити взаємодію громадян з державними структурами. Такі програми, як, наприклад, "План дій щодо електронного урядування" (Action Plan on e-Government) у межах Європейського Співтовариства, мотивували адміністративні органи впроваджувати інформаційні технології у свою щоденну діяльність. По суті, цей План дій представляє собою ініціативу ЄС, розроблену для модернізації цифрових державних сервісів, щоб зробити Європу більш привабливою для економічної діяльності, проживання та вливання капіталу. Ключовою метою цього документа є забезпечення того, щоб кожен житель Європейського Союзу мав повний доступ до переваг, які пропонують цифрові державні послуги.

У цьому, двадцятому першому столітті, бачимо зростання глобальних тенденцій до злиття у сфері електронного урядування. Країни завзято розробляють відповідні плани дій та запускають державні програми, аби збільшити прозорість і покращити ефективність надання послуг у цифровому форматі. Наприклад, Естонія заслужила ім'я новатора у впровадженні саме системи e-Government, пропонуючи громадянам зручні та легкі способи взаємодії з державними установами через електронні платформи.

Щоб осягнути всю сутність електронного урядування, необхідно сфокусуватися на тих фундаментальних схемах, згідно з якими воно реалізується, й оцінити їхні переваги та недоліки.

У нашому дослідженні, а також у відповідних джерелах, виділяють наступні моделі реалізації СЕУ:

1. Єдина модель: Декотрі країни, скажімо, Сінгапур, схиляються до моделі управління, де усі державні сервіси підпорядковані єдиному наглядовому центрові. Сей метод сприяє уніфікованості та ефективному контролю згори, хоча й неминуче ігнорує локальні особливості.

Сильні сторони цього формату включають:

- Впровадження єдиного підходу до адміністрування: Комплексна система полегшує реалізацію електронних послуг, наданих державою, що, як наслідок, прискорює запуск та уніфікацію цих сервісів відповідно до єдиних регламентів.

- оптимізація ресурсів: Зведення до мінімуму повторів функціоналу та надлишкових активів, адже увесь набір електронних послуг постачається через уніфікований хаб.

Однак вона також має деякі недоліки:

- бюрократія: нагода наростання бюрократичних перепон та заплутаних регламентів завдяки системі, сконцентрованій в одних руках;

- обмеженість локальних потреб: може бути менш гнучкою у відповіді на конкретні потреби різних регіонів чи груп населення [40].

2. Децентралізована модель: Приміром, Канада воліє до більш децентралізованої моделі, де органи влади різного рівня оперують власними електронними урядовими засобами. Хоча такий підхід може пропонувати підвищену адаптивність, він водночас накладає більшу потребу у злагодженості дій.

Перевагами такої моделі є:

- гнучкість: модель, що функціонує у децентралізованій формі, здатна краще припасовуватись до унікальних обставин та вимог різнорідних прошарків населення;

- зближеність до громади: забезпечує можливість активно включати громадськість у процеси прийняття рішень та надання послуг [41, 39].

Серед недоліків слід зазначити:
нестандартизація: ризик виникнення різноманітності та

- неоднаковості в реалізації електронного урядування на різних рівнях влади;

ускладнена координація: може виникнути проблема з забезпеченням

- консистентності та ефективної координації між різними адміністративними одиницями.

Глибокий аналіз зазначених сильних та слабких сторін має першочергове значення для визначення найкращого способу впровадження електронного урядування з огляду на особливості певної держави чи територіальної одиниці. Усі рішення зобов'язані брати до уваги унікальні риси менталітету, поточну соціально-економічну ситуацію та запити населення.

У нинішньому світі, дієвість Електронного Врядування (ЕВ) напряму залежить від його організаційного устрою, який гарантує розподіл повноважень та завдань між різноманітними рівнями та секторами управління. Архітектура Електронного Врядування (ЕВ) є багатогранним механізмом, що налагоджує зв'язок між владними структурами та населенням через застосування інформаційних технологій. Ця система охоплює такі елементи:

- Компоненти інфраструктури: Ось складові, що зумовлюють працездатність Системи Електронного Управління. До них належать як елементи, що гарантують захищеність, так і ті, що забезпечують зручність доступу, а також складові для злиття з іншими системами та ті, що стосуються можливості розширення.

- Компоненти послуг: Ось складові, що уможливлюють надання сервісів мешканцям та підприємствам. До них належать елементи, відповідальні за безпосереднє надання послуг, елементи для гарантування якості цих послуг, а також елементи, що забезпечують до них безперешкодний доступ.

Компоненти інформаційної системи: Оце складові, котрі уможливлюють набуття, опрацювання та тримання відомостей. До них належать як ті, що збирають дані, так і ті, що займаються їхньою обробкою, а

також ті, що призначені для зберігання наявної інформації.

Будова Електронного Урядування (СЕУ) може бути різною, залежно від потреб та особливостей певної держави.

У процесі еволюції електронного урядування, спрямованого на інновації, помітну роль відіграють сучасні технологічні досягнення. Ключові компоненти, як-от штучний інтелект, технологія блокчейн, методи аналізу великих даних та системи Інтернету речей, сьогодні є фундаментом для підвищення рівня автоматизованих процесів, зміцнення захищеності та розширення доступу послуг для населення.

Паралельно з цим, міжнародні проєкти активно стимулюють активну участь суспільства у проектуванні та оптимізації електронних урядових систем. Завдяки запровадженню каналів для отримання відгуків, проведенню відкритих обговорень та залученню неурядових структур, досягається принципово новий рівень співпраці між державними інституціями та громадянами.

Охоплення громадян до участі у формуванні та впровадженні електронних урядових послуг (ЕУП) становить ключовий елемент електронного урядування. Так само, як і низка інших держав, Україна залучає населення до розробки та імплементації ЕУП. Конкретно в Україні діє нормативно-правова база, яка обумовлює необхідність залучення громадськості до процесу створення та запровадження ЕУП.

Залучення широкого загалу до етапів формування та реалізації СЕУ можна організувати різноманітними способами, включно з проведенням публічних слухань, а також зустрічами із парламентарями та представниками органів місцевого самоврядування. Аби гарантувати дієву участь громадськості у процесах створення та впровадження СЕУ, в Україні було сформульовано Стратегічні Пріоритети щодо залучення інститутів громадянського суспільства до ухвалення рішень. Розроблення цих пріоритетів здійснювала багатостороння робоча група, а 8 грудня 2014 року у Києві їх представили на круглому столі для обговорення та формування пропозицій щодо подальших кроків. Щойно всі

зацікавлені сторони досягнуть згоди, Рада Європи передасть українській владі "Стратегічні пріоритети залучення громадянського суспільства в процес прийняття рішень", аби ті могли бути інтегровані до Плану Дій Ради Європи для України на період 2015-2017 років.

Всі зазначені елементи містять компоненти функціональних можливостей організації систем електронного урядування, що є важким, насиченим та структурованим процесом. Значне поліпшення роботі органів державної і публічної влади може принести автоматизація адміністративних процесів через використання систем електронного урядування.

Використовуючи систему електронного урядування (СЕУ), можливо поставити на автоматичний рельс чимало управлінських рутинних операцій. До них належать, наприклад, надсилання прохань, оформлення дозвільних документів, реєстрація підприємницької діяльності та подібні справи.

Згідно з даними різних досліджень, коли адміністративні процедури переходять на автоматичні засади, це може спричинити скорочення часових витрат на розв'язання різнопланових завдань. Крім того, спостерігається зниження частоти помилок, які зазвичай виникають через необхідність ручного введення інформації.

Проте, впровадження автоматизації у сфері адміністрування не обходиться без потенційних мінусів. Зокрема, існує ризик скорочення посад, задіяних у виконанні цих адміністративних функцій, а також зменшення прямої комунікації між державними установами та населенням, що, своєю чергою, може негативно позначитися на загальному рівні якості наданих громадянам послуг.

Електроні урядові системи перетворилися на ключовий стратегічний пріоритет для урядів по всьому світу. Протягом останніх років спостерігається стійка тенденція до впровадження та використання таких систем багатьма державами з метою скорочення фінансових витрат, підвищення якості надання послуг, економії часу громадян, а також нарощування продуктивності та

операційної ефективності у державному апараті. Розвиток електронного урядування та поширення мережі Інтернет спричинили глибокі трансформації у соціальній структурі, цінностях, культурних нормах та комерційних практиках, що стало можливим завдяки повноцінній інтеграції потенціалу інформаційно-комунікаційних технологій (ІКТ) у повсякденну діяльність.

Метою електронного урядування є не лише перетворення традиційної інформації в біти та байти та перетворення її у доступну через веб-сайти або надання уряду офіційних комп'ютерів чи автоматизацію старих практик до електронної платформи. Тим не менше, це також вимагає переоцінки методів роботи уряду, того, як наразі виконуються його функції, з метою вдосконалення процесів та забезпечення кращої інтеграції.

Державні органи обидвають у різний спосіб підходи до формування цифрового урядування. Дехто розробляє об'ємні плани на довгий термін, інші ж зосереджуються лише на кількох важливих галузях для початку пілотних ініціатив. У будь-якому випадку, держави, яких вважають найбільш просунутими, розпочинали з менших починань, нарощуючи систему поступово. Науковці, які вивчають цифровізацію урядування, класифікують впровадження за певними періодами чи етапами. Цей матеріал знайомить із різноманітними вивченнями процесу запровадження електронного уряду, що демонструють як корисність розгортання таких систем, так і найсуттєвіші перешкоди, які впливають на реалізацію та подальшу роботу цифрових урядових механізмів.

У цьому контексті доречно згадати поняття "електронна готовність" (або ж "е-готовність"), яке трактується як спроможність держави застосовувати "інформаційно-комунікаційні технології (ІКТ) задля стимулювання економічного зростання та покращення загального добробуту". Паралельно цьому, готовність розглядається як "показник рівня розвитку інфраструктури інформаційних та комунікаційних технологій (ІКТ) та спроможності її кінцевих користувачів — бізнесу та державних структур — ефективно інтегрувати ІКТ на свою користь".

Оціночні показники електронної готовності, кажучи просто, слугують засобами для зважування спроможності держав стосовно запровадження електронного урядування та експлуатації інформаційно-комунікаційних технологій (ІКТ) з метою поступу соціального та економічного характеру. У цих показниках традиційно беруться до уваги різноманітні грані, наприклад, ступінь розвитку інфраструктури ІКТ, наскільки легкою є ця технологія для використання як населенням, так і державними структурами, рівень підключення до мережі Інтернет, а також низка інших важливих чинників.

Скажімо, Індекс електронного урядування від ООН формується, спираючись на певний перелік показників, як-от підключення до мережі Інтернет, можливість для громадян користуватися послугами в режимі онлайн, а також ступінь залучення соціальних медіа. Так само й Світовий банк, до слова, оприлюднює свій індекс е-готовності, котрий вимірює ступінь розвитку електронного урядування в усьому світі.

Скажімо, Індекс електронного урядування від ООН формується, спираючись на певний перелік показників, як-от підключення до мережі Інтернет, можливість для громадян користуватися послугами в режимі онлайн, а також ступінь залучення соціальних медіа. Так само й Світовий банк, до слова, оприлюднює свій індекс е-готовності, котрий вимірює ступінь розвитку електронного урядування в усьому світі.

Існує п'ятирівнева методика, розроблена для оцінки прогресу в електронному урядуванні, яка охоплює еволюцію державних інтернет-ресурсів - від найперших ініціатив до повністю сформованої, згуртованої системи електронного врядування. Спершу ми детально розглянемо кожен із цих етапів:

Етап 1: Поява. На старті свого функціонування влада створює первинну цифрову візитівку, яка складається з низки окремих державних інтернет-ресурсів. Подана там інформація є невеликою за обсягом, не-заглибленою та не динамічною.

Етап 2: Покращення. Веб-портали урядових установ набирають обертів, а

дані у них стають усе більш плинними. Змістовне наповнення та відомості оновлюються з вищою частотою.

Етап 3: Інтерактивність. Користувачі можуть взаємодіяти з урядом через завантаження форм, відправлення електронних листів, планування зустрічей та подання запитів.

Етап 4: Транзакційність. На цьому етапі користувачі можуть фактично здійснювати фінансові транзакції та оплачувати послуги онлайн.

Етап 5: Бездоганність. Досягнення повної інтеграції електронних послуг, яка включає як адміністративні, так і віддільні межі.

Цей підхід визначає порядок розвитку системи електронного урядування від базового рівня до повного використання можливостей електронних технологій для надання послуг громадянам та покращення взаємодії з урядом.

Модель електронного урядування Gartner, розділена на чотири етапи, відображає еволюцію стратегій та функцій електронного урядування. Розглянемо кожен етап більш детально:

Етап 1: Присутність. Це початковий етап, де уряд має простий інформаційний веб-сайт. Веб-сайт може бути пасивним та подібним до брошурного матеріалу.

Етап 2: Взаємодія. На цій стадії стає реальною взаємодія між державними структурами та пересічними громадянами, між урядом і комерційними організаціями, або ж між різними відомствами на державному рівні. Веб-ресурси, властиві цьому етапу, пропонують користувачам електронні адреси для зв'язку та форми, що дозволяють надсилати запити та отримувати потрібні відомості.

Етап 3: Транзакція. На етапі, коли відбувається сама транзакція, користувачам надається можливість здійснювати різноманітні операції у режимі онлайн. Сюди входить, для прикладу, сплата необхідних податків чи отримання ліцензій, або ж подача пропозицій у контексті закупівельних процедур.

Етап 4: Трансформація.Ось найвищий щабель, на якому замислюються

над переглядом функцій урядових структур та самої ідеї керування. Ця зміна передбачає стратегічні зсуви та впровадження електронних засобів задля докорінної перебудови методів обслуговування населення, а також комунікації з громадами та комерційними суб'єктами .

Ключовим моментом є концепція поступового переходу між стадіями, де кожна наступна ланка характеризується збагаченням та розширенням можливостей. Завдяки цій моделі органи влади можуть оцінити поточний стан цифровізації своїх послуг та напрацювати дорожні карти для досягнення вищих рівнів інтеграції, а також покращення комунікації з громадянами та комерційними структурами.

Електронні урядові програми надають громадянам, комерційним організаціям та державним установам можливість цілодобового доступу до урядових відомостей, що, у свою чергу, призводить до підвищення рівня якості цих сервісів.

Запровадження електронного урядування матиме наслідком зниження як фінансових витрат, так і рівня бюрократизації, завдяки впорядкуванню та перебудові діючих робочих порядків. Застосування платформ електронного уряду сприятиме підвищенню продуктивності функціонування державних структур, а також забезпеченню клієнтів публічних сервісів з високою якістю та досягненням поставлених результатів.

Електронне врядування несе вагомі здобутки у плані забезпечення економії та вдосконалення функціонування державних сервісів, що виражається у зростанні ККД, здешевленні операційних витрат, посиленні прозорості дій та розширенні спектру послуг, доступних для населення.

Крім того, визначає наступні переваги електронного урядування:

- Зменшення часу, зусиль і витрат для клієнтів і організацій.
- Покращення надання послуг і задоволення громадян.
- Підвищення навичок користувачів ІКТ, знань Інтернету та використання комп’ютерів.
- Створення нових можливостей для бізнесу та роботи..

Також виявлено багато переваг впровадження електронного уряду, таких як:

- Підвищення ефективності урядових агентств у обробці даних.
- Покращення послуг завдяки кращому розумінню вимог користувачів, що сприяє безперебійній роботі в Інтернеті.
- Обмін інформацією та ідеями між усіма державними установами та відділами для створення бази мега-даних .
- Допомога уряду в досягненні цілей політики через сприяння збільшенню продуктивності, характерної для ІКТ та електронної комерції.
- Підвищення прозорості, точності та полегшення обміну інформацією між урядом і клієнтами.
- Сприяння укріпленню довіри між державними органами та населенням – ключовий елемент ефективного врядування, що досягається завдяки застосуванню онлайн-інструментів. Ці стратегії повинні бути спрямовані на активне залучення громадян до формування політичних рішень, водночас демонструючи урядову відкритість та підзвітність.

На завершення, запровадження електронного урядування не просто обіцяє зекономити кошти, час та робочу силу, воно також має потенціал суттєво покращити якість надання послуг і мінімізувати перебування громадян у державних установах.

Проте, існує низка труднощів та перепон, які можуть сповільнити прогрес у розгортанні електронного урядування. Зважаючи на багатогранність та комплексність проєктів електронного уряду, виникає широкий спектр викликів як на етапі імплементації, так і під час подальшого адміністрування. Далі представлено стислий виклад ключових та найбільш поширених перешкод і труднощів, зібраних на основі аналізу літератури, як це проілюстровано у Таблиці 1.

Таблиця 1

Бар'єри в електронному урядуванні

Категорія	Бар'єри
Технічні	- ІКТ Інфраструктура
	- Конфіденційність
	- Безпека
Організаційні	- Підтримка вищого керівництва
	- Супротив змінам у звичайних
	способах роботи
	- Співпраця
	- Відсутність кваліфікованого
	персоналу та недостатня
	підготовка
Соціальні	- Цифровий розрив
	- Культура
Фінансові	- Високі витрати

Ця таблиця містить зведення ключових перешкод, котрі потенційно можуть проявитися під час розгортання електронного урядування, згрупованих у відповідні розділи. Перехід до електронного уряду затьмарюється суттєвими технічними труднощами, приміром, браком уніфікованих стандартів та єдиної сумісної бази інфраструктури між окремими відомствами й установами. Окрім того, гарантування приватності даних та загальної безпеки постає як визначальний стопор для успішного запровадження електронного урядування в інтересах населення. Лише законодавчого забезпечення з боку влади буде замало, якщо його не доповнити відповідними технічними реалізаціями, прозорими процесуальними нормами і, можливо, незалежним контролем.

Відсутність або недоліки в інфраструктурі ІКТ є однією з ключових труднощів у впровадженні електронного урядування. Щоб належним чином перейти до е-урядування, необхідні архітектурні підходи, котрі охоплюють сукупність засад, зразків та нормативів. Численні країни, що розвиваються, потерпають від цифрової нерівності, яка проявляється як розбіжність в інтернет-доступі між тими, хто його має, і тими, хто позбавлений. Така невідповідність ускладнює впровадження електронного врядування в державах із невеликим рівнем матеріального забезпечення, де технологічні можливості є скінченними.

Забезпечення приватності є надзвичайно важливим питанням як для вже розвинених держав, так і для тих, що знаходяться на етапі становлення, у процесі розбудови електронного урядування. Центральним елементом у питанні конфіденційності виступає гарантування адекватного ступеня охорони відомостей громадян. У сфері е-урядування необхідно вкрай обачно ставитися до збереження особистої таємниці, розв'язуючи проблеми приватності як на технічному, так і на політичному рівнях у межах цієї системи.

Успішна реалізація електронного урядування може наштовхнутися на перешкоди через складнощі у сфері охорони приватності особистих даних. З огляду на питання конфіденційності, що виникають у цифрових мережах, необхідно знайти дієві рішення, аби підвищити рівень довіри серед населення до послуг, що надаються через електронні урядові канали. Для того, щоб впровадження ініціатив електронного урядування увінчалося успіхом, критично важливо гарантувати громадянам впевненість у захисті їхніх особистих відомостей та несення відповідальності за їхнє використання.

Оберігання приватності й захист персональної інформації мусять лишатися на чільному місці у процесі творення та обслуговування веб-ресурсів, де відбувається безпечний збір відомостей. При проєктуванні та втіленні систем електронного урядування необхідно закладати захист приватності на початкових етапах, адже імплантувати його у вже зведену електронну структуру буває надзвичайно складно. Всеохоплюючий політичний документ щодо

конфіденційності має недвозначно окреслювати права громадян стосовно їхньої приватної інформації та накладати обов'язок на органи щодо збереження цих особистих даних, для законних цілей.

Слід мати на увазі, що ІКТ-інфраструктура виходить за межі лише телекомунікаційних мереж та обчислювальних засобів. Аби електронне урядування функціонувало успішно, критично важливими є наявність електронної спроможності та високий рівень обізнаності громадськості у сфері ІКТ. Просвітницька діяльність та забезпечення доступу до знань значно впливають на те, наскільки дієвим буде електронне врядування. Покращення освітніх програм та налагодження партнерства з комерційними структурами здатні стимулювати формування передової інфраструктури, що гарантує рівний доступ до сервісів усім верствам суспільства та окремим громадянам. Таким чином, подолання перешкод, пов'язаних з інфраструктурою, вимагає уваги не лише до технічних питань, а й до не менш значущих освітніх та партнерських складових.

Запуск електронного урядування — це значно більше, ніж просто технічна проблема; це, в першу чергу, організаційне завдання. Серед організаційних складнощів виділяються такі моменти: забезпечення схвалення на найвищому рівні, опір змінам при впровадженні електронних процедур, потреба у стимулюванні взаємодії, а також нестача фахівців потрібного рівня разом із потребою у їхньому навчанні.

- Сприяння з боку топменеджменту: Аби проєкт е-урядування увінчався успіхом, життєво важливо здобути надійну підтримку та активну участь вищого унравляючого складу. Коли така підтримка є значною, це дає змогу виділити потрібні фінансові та людські ресурси, а також гарантує належне стратегічне спрямування для всієї ініціативи.
- Стійкість до змін: Багато електронних ініціатив вимагають переосмислення традиційних процесів та впровадження нових. Стійкість до змін у колективі може утруднити перехід до нових електронних методів роботи.

- Співробітництво та брак кваліфікованого персоналу: Ефективна взаємодія поміж різними департаментами та урядовими установами здатна стати справді складним завданням. Додатково, дефіцит фахівців належної кваліфікації може серйозно завадити успішній реалізації будь-яких електронних проєктів.

- Навчання: Освіта персоналу та постійне навчання є важливими для забезпечення володіння новими технологіями та методами, пов'язаними з електронним урядуванням.

Вирішення цих організаційних викликів є важливим для успішного впровадження електронного урядування та досягнення його максимальної користі .

Суспільні аспекти, котрі стосуються електронного урядування, здебільшого фокусуються на тому, наскільки легкою є його доступність для різноманітних верств населення. Це, по суті, означає розробку інтерфейсу, яким зможе користуватися будь-яка особа, що потребує державних сервісів. Серед соціальних труднощів можна окремо виділити низку чинників: нерівномірність доступу до цифрових технологій, відмінності у культурному середовищі, ступінь досвідченості громадян та їхні фінансові можливості. В межах нашого обговорення ми детальніше зупинимося на двох із цих аспектів: нерівності у використанні технологій та культурних відмінностях.

- Цифровий розрив: Однією з головних проблем, що постають на шляху розгортання електронного урядування, є цифрове розмежування поміж тими, хто користується мережею Інтернет та сучасними цифровими засобами, та тими, хто цього позбавлений. Така нерівність у доступі здатна спричинити поглиблення соціальної нерівності та обмежити для певної частини суспільства здатність повноцінно скористатися перевагами, що надаються урядовими електронними сервісами.

Культурні особливості: Особливості національних ментальностей та звички можуть створити певні труднощі на шляху до впровадження системи

електронного урядування. Наявність різних мов, розуміння важливості певних

- аспектів та пристосування до різних культурних контекстів може вплинути на ефективність та прийняття електронних урядових послуг. [48, 49]

Резюмуючи вищевикладене, цей розділ деталізує різні стадії розгортання е-уряду, акцентуючи увагу як на позитивних аспектах, так і на потенційних труднощах, що можуть стати на заваді успішній імплементації електронного урядування. Очевидно, що електронний уряд розвивається поетапно, пропонуючи значні вигоди для державного апарату, населення та підприємницьких кіл. Проте, реалізація е-уряду – це нетривіальне завдання, що наштовхується на низку складнощів та перепон, які потребують ретельного аналізу та подолання.

2.2 Значення систем управління інформацією у вдосконаленні процедур державного управління.

Дієвість, з якою працює система державного нагляду та контролю, демонструється через реалізацію запроваджених вердиктів у секторах господарства, суспільного життя та довкілля. Дана теза є основоположною засадою у злагодному оновленні механізмів виконавчої влади, мета якого — наростити результативність роботи урядових інституцій як на рівні далекосяжного планування, так і на етапі щоденного виконання завдань.

Проте ключовим є здатність визначати та фахово оцінювати цю дієвість, спираючись на чітко окреслені та реально впроваджувані показники. На жаль, у наш час відсутня універсально визнана парадигма щодо того, як саме конструювати критерії та проводити вимірювання результативності роботи державних структур. Ба більше, бракує стандартизованих методологій чи усталених внутрішніх регламентів, які б дозволяли здійснювати неупереджену експертизу.

З огляду на це, формування стрункиx критеріїв та узгоджених методологій, які адекватно відображають реальні вимоги, постає як першочергове завдання.

Важливо дослідити та імплементувати свіжі парадигми для зважування результативності механізму державного керування, добиваючись при цьому неупереджених та вагомих висновків, що слугуватимуть фундаментом для майбутніх планів та виконавчих дій.

У теоретичних надбаннях бачимо цілу низку парадигм для визначення результативності керівних процесів, серед яких виділяються метний (цільовий), операційний (функціональний), складовий (композиційний), етичний (поведінковий) та низка інших. Зважаючи на сутнісні особливості адміністративної роботи у сфері державного врядування та управління, найрелевантнішою методологією, що фігурує у фаховій літературі, визнається метний (цільовий) спосіб оцінювання.

Даний метод спирається на концепцію, згідно якої ключове завдання будь-якого механізму координації у відповідних галузях полягає у досягненні визначених завдань найбільш обґрунтованим шляхом. Таке цілеспрямоване бачення нерідко інтегрується із засобами визначення результативності, що формуються на основі аналізу поведінки, чиї регламенти ґрунтуються на фіксації досягнення гармонії інтересів усіх стейкхолдерів у підсумках роботи державних органів.

Цей показник вважається головним при аналізі результативності функціонування державного сектору й слугує основою для системи метрик, що дозволяє з’ясувати, наскільки виконані намічені завдання. Для з’ясування цього застосовують як методи безпосереднього обчислення, так і підходи непрямої оцінки, зокрема, залучення фахівців, опитування респондентів та інші подібні.

У процесі вдосконалення державного управління та підвищення якості надання суспільних послуг, злиття систем інформаційного управління має першорядне значення для досягнення оптимальних результатів, як наголошується у джерелі. Ключові елементи, що становлять цю інтеграцію, охоплюють:

- Оптимізація робочих процесів: Інтеграція інформаційних систем

дозволяє автоматизувати та уніфікувати різноманітні адміністративні процеси.

- Це сприяє ефективному використанню ресурсів, скороченню часових рамок та уникненню зайвої бюрократії.

- Покращення доступу до інформації: Зведення докупи розрізнених інформаційних платформ дає змогу унаочнити процеси збереження та роботи з даними в єдиному осередку. Завдяки цьому різноманітні органи влади отримують спрощений доступ до потрібної інформації, що, у свою чергу, веде до оперативного й безпомилкового формулювання управлінських рішень.

- Підвищення координації та взаємодії: Зведення до купи (інтеграція) систем керування, що наявні, веде до суттєвого покращення як внутрішнього обміну даними, так і міжсекторної взаємодії. Завдяки цьому різноманітні структурні підрозділи та управлінські рівні отримують змогу плідно працювати спільно, аби розв'язувати спільні проблеми та реалізовувати визначені наперед стратегічні накреслення.

Забезпечення прозорості та відкритості: -Об’єднання різноманітних систем провадить до формування спільного середовища, де державні установи та населення можуть обмінюватися даними. Такий підхід посилює відкритість у процесі ухвалення урядових рішень і водночас заохочує активнішу комунікацію між адміністрацією та суспільством.

- Підвищення безпеки даних: Зведення до купи належних систем дає змогу ґрунтовно розпоряджатися та охороняти чутливі дані. Така спроможність є ключовою для підтримання належної захищеності та відповідності усім чинним нормам.

Щодо фундаментального визначення, інформаційна система (ІС) являє собою сукупність скоординованих дій, спрямованих на опрацювання даних, що спираються на відповідні організаційні активи: людський капітал, технологічне забезпечення та фінансові ресурси, мета яких — постачання та розповсюдження відомостей. Взаємозв'язки між складовими елементами та їхня взаємодія із зовнішнім контуром забезпечуються через інформаційний обмін. Будь-яка ІС за

своєю суттю містить сховище даних (базу даних) та набір програмних засобів, які надають різним категоріям користувачів можливість оперувати даними цього сховища, тим самим сприяючи виконанню ними поточних робочих функцій.

Виходячи з цього, інформаційна система являє собою комплекс прийомів, технологій, методик та регламентів, призначених для акумуляції, прогнозування, підготовки, транспортування, збереження й опрацювання відомостей, а також для розповсюдження та візуалізації даних з метою ухвалення рішень.

Активний поступ інформаційних систем бере свій початок із запровадженням електронно-обчислювальних машин та іншого устаткування, призначеного для опрацювання ділової інформації, яку доти доводилося робити це вручну. Становлення інформаційних систем ґрунтується на певних засадах, має свої обмеження та рушійні сили; на часі ж такими основами для виведення концепцій проєктування інформаційних систем слугують системна теорія та інформатика. Системи, де у цій сфері застосовуються обчислювальні машини й інформаційні технології (IT), іменують комп'ютерними інформаційними системами (CBIS). Суть роботи інформаційної системи полягає у трансформації початкових даних у вихідну інформацію, яка стане придатною для ухвалення рішень.

Отримана інформація слугує інструментом для верифікації відповідності отриманого результату фактичному стану справ. У випадку, коли фактичний показник розбігається з прогнозованим результатом, здійснюється аналіз та внесення змін до вихідних умов.

Часто трапляється, що дані, які вводяться у комп'ютер, містять неточності, і це, як правило, є результатом людської неуважності чи стомленості, що спрощує їхнє усунення. Натомість, програмні збої можуть мати коріння у внутрішній складності самої програми, яка іноді сягає таких масштабів, що розробник фізично не в змозі охопити увесь її обсяг контролем.

Навіть коли цілком очевидно, що десь у коді криється хиба, локалізація цієї проблеми та її подальше виправлення перетворюються на надзвичайно складне

завдання. Потім, після того, як дефект знайдено та усунуто, існує немала вірогідність, що це нововведення може зачепити роботу інших модулів системи, аж до того, що виникне новий, можливо, критичний для функціональності програми баг.Для того, аби впоратися з труднощами, які виникають завдяки складності програмних систем, необхідно спершу створити таку їхню будову, яка буде зрозумілою для програміста (це, власне, означає впровадження принципів структурного підходу при розробленні програм).

Структура програми має бути організована у формі модулів, що характеризуються певною автономністю, що дає змогу проводити їх опрацювання ізольовано, без залежності від решти елементів (ідеться про застосування принципу модульності під час створення програми).

Центральною складовою будь-якого "пакету реформ", що спрямований на трансформацію, виступає перебудова державного сектору. Така перебудова має критичне значення, проте її впровадження пов’язане зі значними труднощами. На це вказує досвід, набутий Сербією. Під кінець 2003 року Агентство Сербії з питань розвитку державного управління звернулося до норвезької державної фірми Statskonsult із замовленням на підготовку аналітичного звіту стосовно реформування державного управління в Сербії. Фінансування цього дослідження, яке охоплює п'ять основних секцій, було схвалено завдяки підтримці МЗС Норвегії. Згадані секції мають назви: "Передумови реформи: наслідля та складні питання", "Характеристика реформи: успіхи та прорахунки", "Оціночні судження щодо реформи", "Аргументація реформи", а також "Адаптація реформи". Дослідження також містить чотири ґрунтовні додаткові матеріали, що є його невід’ємною складовою.

Було проведено аналіз трьох взаємопов'язаних тем: ступінь успішності впровадження реформи державної служби у Сербії за період 2001–2004 років (до березня 2004 року, коли розпочав роботу новий уряд); які чинники сприяли цій реформі та які створювали бар'єри; а також чи потребує програма та сам хід реформування змін, і в якому напрямку ці зміни мають відбуватися?Для відповіді на кожне з цих питань автори

дослідження, Свейн Еріксен і Даг Солумсмоен, використовували три групи даних: опубліковані матеріали, інтерв'ю з ключовими особами, що приймають рішення, і дані, отримані в результаті дослідження, в якому взяли участь всі державні службовці з п'яти міністерств. У цьому дослідженні автори сконцентрувалися на трьох величинах, які є першорядними у наукових працях щодо трансформацій інституцій у країнах Центральної та Східної Європи. Ці змінні - "структура" (реальна спроможність інститутів у розпорядженні керівництва держави), "вплив лідерів" та "зовнішні чинники" - слугували підґрунтям для верифікації успішності реформування державного апарату в Сербії. Для цього було залучено дві групи інформації: експертні оцінки безпосередніх учасників або спостерігачів процесу реформування, а також зіставлення динаміки нарощування загального адміністративного ресурсу Сербії з показниками Словенії, Хорватії та Македонії.

Обмеженими можна вважати здобутки реорганізації державного сектору в Сербії. На думку авторів, найвагомішим успіхом за цей час стала суттєва зміна персоналу. Проте, з'явилися певні труднощі. За три роки конституційний устрій набув складностей, а розмежування між юридичними нормами та політичними процесами стерлося. Окрім того, сербські відомства являють собою централізовану бюрократичну структуру, де пріоритетом є нагляд і ухвалення рішень за принципом "згори донизу". Керівна ланка та організаційна побудова спричинили негаразди та обмежили потенціал реформаторської діяльності. Лідерство справило згубний вплив через свою роз'єднаність та перенапруження уваги й ресурсів на інші сфери. Сама структура виявилася непридатною для формування спроможності в галузі узгодження дій, взаємодії, обміну інформацією та вироблення політик. Зовнішні чинники, зокрема фінансова підтримка від донорів, здебільшого справляли сприятливий вплив на адміністративні реформи, однак це становило лише необхідний, а не вирішальний етап для формування нових перспектив. Остаточна теза цього звіту полягає у констатації слабкості державного апарату Сербії, що проявляється у

браку належної взаємодії між різними відомствами. Отже, ключовим завданням є посилення координації та обміну інформацією шляхом ретельно виважених кроків, аби забезпечити прогрес у сферах інновацій та формування державної політики.

Поняття "інформаційна система" знаходить застосування у різноманітних сферах, набуваючи різних тлумачень. Згідно з нормативним актом "Про інформаційну систему управління людськими ресурсами у державних органах", який був затверджений постановою Кабінету Міністрів 28 грудня 2020 року, під інформаційною системою розуміється програмно-технічний комплекс, призначений для збору, опрацювання, збереження та охорони відомостей щодо персоналу органів виконавчої влади. Цей комплекс розгортається та експлуатується відповідно до встановлених законодавством вимог з метою підтримання єдиного електронного реєстру співробітників державних установ, а також для запровадження автоматизованих та цифровізованих засад управління кадрами та нарахування винагороди. Сам цей розпорядчий документ окреслює регламент функціонування системи управління людськими ресурсами в держструктурах як програмно-технічний комплекс для накопичення, обробки, зберігання та захисту даних у сфері державної служби.

У сфері державного та публічного управління, ця система функціонує з огляду на досягнення таких завдань:

- Формування уніфікованого сховища даних стосовно осіб, зайнятих на державній службі та в інших уповноважених структурах.
- Впровадження автоматизованих та цифровізованих рішень у сфері управління персоналом у державних структурах, що відповідають за формування та ухвалення кадрових рішень.
- Оцінка ефективності роботи структурних одиниць, відповідальних за кадрове адміністрування.
- Гарантування публічності та зрозумілості відомостей стосовно особового складу та винагороди за працю у відповідних виконавчих структурах.

- Зміцнення потенціалу відділів кадрів та фінансового обліку у виконавчих органах.
- Сьогоденна еволюція менеджменту людських ресурсів зумовлюється спроможністю системи забезпечувати оперативний збір, валідність, вичерпність, легкість доступу, гнучкість опцій та стійкість процесів обліку, опрацювання, кумуляції, трансферу та візуалізації відомостей у царині державного сектору.
- Робота системи електронної інформації на державній службі й обмін даними між державними електронними інформаційними джерелами стосовно адміністрування персоналу.
- Електронна взаємодія між органами впровадження.
- Забезпечення співробітників органів, що реалізують проєкти, доступом до відомостей шляхом використання особистого електронного кабінету в інформаційній системі, призначеної для електронної комунікації з відділами та іншими фахівцями цього органу, що впроваджує.

Усвідомлюючи, що системи керування даними вже закріплені у вітчизняному законодавчому полі, необхідно акцентувати увагу на їхній незамінній функції у досягненні високої продуктивності та раціоналізації процедур у царині державного управління та муніципальних служб. Значущою є теза про те, що потреби у створенні окремих додаткових регуляторних документів для цього не існує, що має вирішальне значення для правильного сприйняття та фактичного впровадження означених електронних систем.

Новітній спосіб керування, який нині активно впроваджується як Київською міською радою, так і міською державною адміністрацією, ставить за мету раціоналізувати процедури в межах державного та публічного адміністрування. Зважаючи на розвиток соціуму, необхідною стає інтеграція технічних інновацій задля полегшення роботи у всі сферах, особливо з огляду на пандемічну ситуацію, яка змусила органи влади та місцевого самоврядування трансформувати свої робочі формати, перейшовши переважно на дистанційний

режим діяльності.

Міська рада міста Києва, як орган самоуправління на місцях, завзято запроваджує новітні технології для підвищення результативності своєї діяльності. Депутати дев'ятого скликання послідовно застосовують дистанційний формат, проводячи голосування в електронний спосіб на сесіях та завдяки застосуванню електронно-цифрового підпису. Для оптимізації функціонування міської ради було створено відповідний мобільний додаток.

Столична державна адміністрація, у зв'язку із запровадженням карантинних обмежень, організувала свою роботу у віртуальному форматі, де переважна частина персоналу трудилася дистанційно. Завдяки електронним системам управління документами, які були інтегровані ще до настання пандемії, цей орган місцевого самоврядування зумів зберегти безперервність функціонування та успішно трансформувався у напрямку новітніх методів організації праці. Подібні підходи залишаються життєво важливими й у нинішній ситуації протистояння російській навалі.

Однак, окрім суто організаційних моментів, ключовим елементом у сучасному керівництві виступає сама суть роботи. Нинішня Київська міська державна адміністрація інтенсивно впроваджує електронні методи керування з метою раціоналізації міського середовища. Центральну роль у цьому механізмі відіграє Департамент інформаційно-комунікаційних технологій, що є складовою виконавчої влади Київської міської ради. Саме цей структурний підрозділ встановлює необхідність формування електронних сховищ даних та інформаційних систем, що є пре-реквізитом для формування уніфікованого інформаційного поля громади міста.

Зокрема, на нього покладено завдання щодо створення, розвитку, обслуговування та гарантування інформаційної безпеки електронних ресурсів даних та баз відомостей. Крім того, він відповідає за узгодження та надання методичних вказівок органам влади як центрального, так і місцевого рівня у межах Києва, а також суб'єктам господарювання, установам та організаціям у

питаннях запровадження інформаційних технологій, телекомунікаційних мереж та рішень, електронного врядування, захисту даних та інших ключових сфер діяльності.

Правова база України не просто надає згоду, а й рішуче мотивує державні інституції, органи виконавчої влади та комерційний сектор до пришвидшеного запровадження інформаційних технологій. Ця імператива закріплена як на рівні законодавства, так і через запуск низки цільових ініціатив. Зокрема, Закон України "Про Національну програму інформатизації", ухвалений під кінець 2022 року, інтерпретує національну програму інформатизації як сукупність завдань, проєктів та робіт, спрямованих на інформатизацію. Подібні кроки мають на меті стимулювання формування інформаційного суспільства через фокусування та ефективне використання коштів, матеріальних засобів, а також науково-технічного та виробничого потенціалу країни. Згадана Програма передбачає узгодження дій між представниками влади різного рівня (державної та муніципальної), а також суб'єктами господарювання, незалежно від їхнього організаційно-правового статусу.

У межах Національної програми інформатизації, одне з ключових завдань полягає у відображенні тієї фундаментальної ролі, яку відіграють інформаційні системи управління у вдосконаленні як державних, так і процесів, що стосуються сфери публічного адміністрування.

Вона спрямована на забезпечення:

- Створення, запровадження та використання засобів інформаційно-комунікаційних технологій у роботі державних органів, органів місцевого самоврядування та у сфері громадського життя;
- здійснення проєктів та запровадження кроків, призначених для розбудови електронного урядування та демократичних електронних процесів;
- формування та вдосконалення системи державних інформаційних надбань;
- удосконалення процедури надання публічних (електронних

публічних) послуг;

- забезпечення електронного документообігу з метою налагодження інформаційного обміну між державними установами та органами муніципального управління;
- розробка інформаційно-аналітичних комплексів для урядових та муніципальних установ;
- оптимізація продуктивності відчизняних фабрик через імплементацію інфокомунікаційних та діджитал інструментів;

Аби міські та селищні ради працювали краще, критично необхідно запроваджувати сучасні цифрові рішення. Проте, на цьому шляху розвитку є низка перешкод, які сповільнюють прогрес, а саме:

- Брак належного обсягу та рівня комп'ютерного оснащення: Річ у тім, що в чималій кількості населених пунктів нашої країни - як у великих містах, так і в селищах - фахівці досі стикаються із ситуацією, коли наявна апаратура не відповідає актуальним технологічним стандартам.
- Невідповідність апаратури потребам праці: Застосування невідповідного знаряддя спричиняє його швидке псування, а якщо немає запасної апаратури, виконання завдань стає утрудненим.
- Слабка кваліфікація персоналу: Недостатній рівень володіння потрібними уміннями для роботи із софтверним пакетом створює ґаджета для виконання завдань.
- Бракує україномовного варіанту: Немає перекладу для програм, що існують іншими мовами, формуючи мовний прошарок, який згубно позначається на продуктивності праці.
- Недостатнє забезпечення коштами становитиме центральним викликом у становленні інформаційно-комунікаційного потенціалу муніципалітетів.

Для вирішення цих проблем можна акцентувати увагу на наступних заходах:

- Придбання спеціальної комп’ютерної техніки: Необхідно передбачати виділення коштів на обладнання та забезпечення органів місцевого самоврядування резервною технікою в місцевих бюджетах.
- Освітня робота: Організація тренінгів для чиновників та представників органів місцевого самоврядування, спрямованих на ознайомлення їх із новітніми інформаційними технологіями з метою підвищення загального рівня їхньої компетентності.
- Впровадження електронних систем документообігу: Уведення подібних систем стимулює оперативне залагодження питань, що стосуються місцевого самоврядування, забезпечує ефективне використання коштів місцевого бюджету та впорядкування документації у владних структурах на місцях.

Хоча впровадження інформаційних технологій і створює певні труднощі, його переваги для муніципалітетів та покращення обслуговування мешканців є очевидними. Лише уважне ставлення до цих моментів гарантуватиме дієвість та модернізацію адміністративного управління на місцях.

Висновки за розділом 2

У рамках цього розділу було проведено глибокий аналіз впровадження інформаційних технологій у сферу державного управління. Детально розглянуто архітектуру, структуру та функціонал платформ електронного урядування, а також з'ясовано, як інформаційні системи впливають на вдосконалення управлінських процедур у державному секторі.

Стосовно систем електронного урядування, ключовим моментом є те, що їхнє проєктування та адміністрування задають вектор розвитку відносин між державними інституціями та населенням. Наголошується, що розробка таких систем є надзвичайно важливою для забезпечення прозорості та зручності адміністративних послуг. Функціональні можливості цих систем розглядаються як необхідні для автоматизації та поліпшення роботи державних структур, що

сприяє оптимізації їх функціонування.

Аналіз функцій систем управління інформацією довів, що інтеграція подібних рішень є життєво важливим кроком для покращення скоординованості й результативності у сфері адміністрування. Констатується, що ці інфосистеми не просто дають змогу провадити ефективний збір та аналіз відомостей, а й спрощують механізми ухвалення рішень, гарантуючи водночас значну швидкість реагування. Введення в дію таких систем розглядається як ключовий елемент для формування гнучких та пристосованих структур управління, які відповідають актуальним потребам сьогодення.

Таким чином, акцентується увага на значущості інформаційних інструментів у державному управлінні, вказуючи на їхній спроможний потенціал для кардинальної зміни управлінських методик та досягнення високого ступеня дієвості й налагодженої комунікації між владними інституціями та населенням.

3 ГАРАНТУВАННЯ ІНФОРМАЦІЙНОЇ СТІЙКОСТІ ПРИ АКТИВНОМУ ЗАСТОСУВАННІ НОВІТНІХ ІНФОРМАЦІЙНИХ ЗАСОБІВ

3.1 Загрози та небезпеки у сфері інформаційної безпеки в державному секторі.

Немає жодного відкриття в тому, що знання (інформація) у наш час перетворилися на провідний актив, і питання гарантування захищеності цих відомостей у сфері державного управління набуває надзвичайної ваги. Збільшення кількості даних, які підлягають електронній обробці, та ширше застосування ІТ у роботі державних структур тягне за собою зростання потенційних небезпек та вразливостей, здатних позначитися на продуктивності та захищеності державних інституцій. Таким чином, оволодіння знаннями про ці загрози та оцінка ризиків у сфері захисту інформації стають імперативом для зміцнення довіри та сталості державного апарату перед викликами, що постають із кіберпростору. У цьому контексті необхідно бачити цю проблему як фундаментальний елемент планування роботи з інформаційними активами та гарантування їхньої недоторканності у межах нинішнього цифрового ландшафту.

Забезпечення інформаційної стійкості у сфері державних послуг являє собою сукупність кроків, котрими прагнуть гарантувати нерозголошення, достовірність та можливість використання відомостей, що проходять обробку та зберігання у державних керуючих архітектурах.

Глава Української держави, Володимир Зеленський, ввів у дію ухвалу Ради національної безпеки й оборони України датовану п'ятнадцятим жовтня дві тисячі двадцять першого року, що має назву «Про Концепцію інформаційної безпеки». Цей стратегічний документ окреслює поточні проблеми та небезпеки для державної безпеки України у сфері інформації, стратегічно важливі амбіції

та необхідні дії, націлені на протистояння цим викликам, оберіг юридично закріплених прав громадян стосовно доступу до відомостей та захист персонально ідентифікованих даних .

Кібератаки є лейтмотивом серед загроз для інформаційної безпеки у державному секторі. Як засвідчують дані CERT-UA, лише за перші три місяці 2023 року обсяг кіберзлочинності в Україні підскочив на шістдесят п’ять відсотків, що наочно демонструє гостроту питання. Збільшення кількості кіберзлочинів також корелює з неприйнятно високим інтересом з боку хакерських угруповань держави-агресора. Це найчастіше виражається у нападах на інфосистеми відомств, пов'язаних із обороною та державним управлінням, а також у невпинних спробах несанкціонованого втручання у функціонування систем електронного зв'язку та об'єктів життєво важливої інфраструктури країни.

З огляду на викладене, інформаційну безпеку слід розглядати не лише крізь призму технічних рішень, але й як багатогранну архітектуру, що охоплює дієві законодавчі, управлінські та технологічні превентивні заходи. Важливість імплементації цих заходів закріплюється на тлі невпинного технологічного прогресу та експансії різноманітних кібернетичних небезпек.

Інформаційна безпека у державному урядуванні являє собою цілісний метод захисту даних від усього спектру потенційних ризиків, гарантуючи безперебійну роботу урядових інституцій. Успішна реалізація цього імперативу вимагає синергії нормативно-правових кроків, застосування новітніх технологій та освітніх програм с метою досягнення високого рівня захищеності інформації та підтримки громадянами довіри до органів влади.

На органи влади, як на державному, так і на місцевому рівнях, лягає відповідальність за належне функціонування суспільства; при цьому їхні завдання дедалі більше спираються на інфраструктуру інформаційних технологій та процеси керування даними. З огляду на зростання обсягів цифровізації урядових та комунальних структур - зокрема, впровадження електронного урядування, ведення реєстрів громадян та адміністративних

процесів, а також надання послуг через мережу - інформаційні активи набувають критичного значення.

Тим не менш, охорона відомостей у представницьких та самоврядних установах є життєво необхідною для підтримки таємності, неушкодженості та зручності оперування відомостями. Збереження таємниці гарантує убезпечення від небажаного ознайомлення з чутливими даними, як-от персональна інформація мешканців чи стратегічні задуми. Непорушність даних (цілісність) є важливою для підтвердження того, що відомості не зазнають несанкціонованих трансформацій чи знищення, забезпечуючи цим самим вірогідність наявної інформації. Водночас, можливість отримання (доступність) виступає вирішальною умовою для безперервності функціонування державних органів та забезпечення доступу до потрібних відомостей у будь-який час.

Запотреба у дієвому захисті інформаційних активів диктується не лише внутрішніми імперативами держави, але й зобов'язаннями, що випливають із відносин із населенням. Державні інституції оперують колосальними масивами персональних відомостей та конфіденційної документації, відповідно, на них покладено відповідальне завдання щодо їхнього надійного зберігання. Невдача на цьому терені здатна спричинити не лише технологічні ускладнення, а й підірвати громадську довіру, що суттєво позначиться на владній вертикалі та її легітимності.

Слід наголосити: у воєнний час відомості, що охоплюють конфіденційну інформацію, виступають вирішальними для визначення основних кроків як у загальному розвитку подій на світовій політичній сцені, так і безпосередньо на зоні бойових дій. Багато визначних звершень українських спецслужб, націлених на поразку супротивника, не відбулися б, якби не були суворо дотримані вимоги до збереження та обміну даними як у межах самих органів, так і за їхніми межами.

Оглянемо ключові ризики для безпеки інформації у державному секторі.

Кібератаки. Кібератаки стають все більш виразним викликом для державних інформаційних систем, оскільки сучасні технології розвиваються, а

кіберзлочинці використовують все більше та більше удосконалених методів для впливу на державні структури. Попереднє розуміння ознак та наслідків кібератак є критично важливим для впровадження ефективних заходів забезпечення інформаційної безпеки в публічному секторі.

Кібератаки мають безліч методів і способів вчинення, що і складає основу такого поняття як - кіберзлочинність загалом.

Для зрозумілості, ми можемо надати своє бачення у класифікації кіберзлочинних дій, що можуть впливати на публічний сектор:

- Поширення вірусів, троянських програм, хробаків та інших зловмисних програмних засобів: з метою здобуття незареєстрованого доступу чи спричинення руйнування.
- Шпигунство у кіберпросторі: застосування софту з метою видобутку чутливих даних, на зразок облікових даних доступу, криптографічних ключів і подібного; заходи, націлені на незаконне викрадення відомостей із комп'ютерного обладнання та мережевих інфраструктур.
- Кібертерор: масове надсилання запитів з метою перенасичення серверів та унеможливлення доступу до ресурсів (DDoS-атаки); спроби втручання у роботу об'єктів критичної інфраструктури, як-от енергомережі, транспортні вузли, і таке інше.
- Психологічний тиск та маніпуляції: застосування оманливих електронних послань чи фальшивих інтернет-ресурсів з метою видобутку чутливих даних (фішинг); залучення психологічних прийомів для несанкціонованого доступу до відомостей.
- Кіберконфлікт: застосування комп'ютерних інструментів у проміжку бойових дій з метою здобуття відомостей та ураження інформаційних структур противника.
- Кіберекономічні атаки: використання Інтернету для здійснення фінансових злочинів, таких як крадіжка грошей, використання банківських карт тощо.

- Кібератаки на людей: спроби використання або крадіжки ідентифікаційних даних користувачів.

З-поміж іншого, варто згадати про ще один різновид кіберзагроз, появу якого зумовила відкритість та повсюдне поширення інформації в мережі. Інформаційно-психологічні операції (ІПСО) — це заходи, мета яких полягає у донесенні певних відомостей та сигналів до цільової аудиторії з розрахунком на те, щоб змінити її спонукальні мотиви, раціональні оцінки, а отже, і дії урядів, установ, об'єднань та значних іноземних держав.

Ця форма кібератак залучає психологічні підходи для формування поглядів, переваг та взаємозв'язків між різноманітними акторами у віртуальному просторі. ІПСО може охоплювати поширення неправдивих даних, маніпулювання діяльністю у соціальних мережах, фабрикування підроблених особистостей та застосування інших методів для формування певного враження чи чинення тиску на суспільну думку.

Вплив кібератак на державні інформаційні системи:

- Злом особистих даних: Кібератаки здатні спричинити розголошення приватної інформації, що ставить під сумнів авторитетність та безпеку систем.
- Втрата доступності: Напади можуть призводити до відмови в обслуговуванні (DDoS), що забезпечує неможливість доступу до інформаційних ресурсів.
- Пошкодження цілісності: Злочинці можуть змінювати або пошкоджувати інформацію, що може призвести до невірного прийняття рішень на рівні влади .

Наприкінці квітня 2022 року, оприлюднена доповідь від відділу кібербезпеки корпорації Microsoft (Digital Security Unit) розкрила деталі російської кіберактивності, що супроводжувала повномасштабне вторгнення в Україну. Дана публікація стала можливою завдяки спільній роботі Microsoft із суб'єктами кібербезпеки як урядового, так і приватного секторів України.

Згідно з опублікованим документом, діяльність російських хакерів переважно була спрямована на компрометацію об'єктів по всій території України.

Ці дії охоплювали два основні етапи: спершу проводилися фішингові операції задля здобуття доступу до внутрішніх мереж цілей, а вже потім наголос робився на знищенні чи зміні даних, паралельно із здійсненням операцій кібершпигунства.

Протягом періоду з двадцять третього лютого до восьмого квітня дві тисячі двадцять другого року було зафіксовано мінімум сорок успішних кіберінцидентів, що спричинили ушкодження файлів у сотнях систем, задіяних у діяльності десятків українських установ. Було задіяно щонайменше вісім різних сімейств вірусів, призначених для перезапису та видалення інформації, виведення з ладу комп'ютерних систем та втручання у роботу систем керування промисловими процесами (ICS). Сорок відсотків актів руйнування (деструктивних атак) були націлені на об'єкти критичної інфраструктури (ОКІ), що здатне негативно позначитися на державному управлінні, військових структурах, економіці та цивільному населенні. Тридцять два відсотки інцидентів стосувалися державних інституцій України різного рівня.

Корпорація Microsoft пов'язала ці хакерські угруповання з ключовими російськими службами безпеки: Федеральною службою безпеки (ФСБ), Головним розвідувальним управлінням (ГУ ГШ ЗС РФ) та Службою зовнішньої розвідки (СЗР РФ). Стає очевидним, що російські хакери готувалися до військової агресії проти України не менше, ніж із березня дві тисячі двадцять першого року, що виливалося у фішингові кампанії та спроби кібератак через ланцюжки поставок.

Звіт також акцентує увагу на гнучкості російських зловмисників, які оперативно вносять зміни у свої віруси, щоб ускладнити їхнє виявлення. З поглибленням протистояння зростає ймовірність виявлення деструктивного шкідливого програмного забезпечення. Зазначається, що ті, хто здатний підтримувати такий високий темп адаптації, становлять суттєву небезпеку, а їхні дії можуть набути ще більш руйнівного характеру.

Згідно з висновками цього дослідження, подальший розвиток конфлікту може спричинити застосування резервних (запасних) потенціалів, таких як

використання невідомих досі вразливостей ("нульового дня"), цілеспрямовані атаки на критично важливі об'єкти та кібервтручання через ланцюжки постачання. Зростання обсягів технічного сприяння Україні здатне підштовхнути російських кіберзлочинців до експлуатації вразливостей "нульового дня", що, своєю чергою, може стати небезпекою для установ у глобальному масштабі.

Згідно з ухваленим документом, прогнозується, що ворожі кібернетичні наступи сфокусуються насамперед на телекомунікаційних мережах України, зокрема на провайдерах інтернет-послуг. Російське керівництво планує розгорнути свої кібероперації на більшу кількість територій, приділяючи особливу увагу країнам, які надають допомогу українській стороні. Цей арсенал заходів охоплюватиме як добування інформації через мережевий простір, так і здійснення актів кібернетичного руйнування.

У тому ж самому документі наведено типовий перелік методів та тактик, які застосовують російські зловмисники, а також надано дієві настанови для команд кіберзахисту щодо мінімізації загроз від деструктивних кібератак. З огляду на викладене, варто особливо підкреслити критичну важливість посилення заходів захисту інфраструктури та постійного вдосконалення підходів до кіберзахисту.

Спостерігається чітка закономірність: кіберконфлікт під час розгортання активних бойових дій постає як надзвичайно серйозне випробування для сфери кібербезпеки, що зумовлює необхідність найвищого рівня компетентності та підзвітності для всіх суб'єктів – як державних структур, так і приватного сектору.

Злив секретних даних становлять докорінну небезпеку для державних структур та широкого загалу, здатну мати згубні відбитки на обороноздатності країни та приватному житті громадян. Проаналізуємо, які різновиди й шляхи цього витоку бувають, якими є їхні наслідки та які кроки можна вжити для їхньої профілактики.

Різноманітність форм та способів несанкціонованого розголошення

службової таємниці значною мірою, хоч і частково, зумовлюється тими складниками, що спричинили цей інцидент. Перш за все, сам факт витоку даних, як він себе являє, є прямим наслідком або фінальним результатом тих кібератак і злочинних діянь у цифровій сфері, що були згадані раніше.

Наслідки для урядових органів та громадськості:

- Втрата довіри: Злиття секретних даних здатне спричинити підрив довіри громадян до державних інституцій та посилити небезпеку поширення корупційних практик.

- Безпекова загроза: Злив таємних даних, а особливо тих, що стосуються оборони та безпеки, здатний спровокувати акти агресії чи тероризму.

Всі напрямки потенційного витоку конфіденційної інформації можна класифікувати як непрямі та прямі. Непрямі канали характеризуються відсутністю необхідності безпосереднього доступу до технічних засобів інформаційної системи. Натомість, прямі канали забезпечують безпосереднє потрапляння до апаратної бази та сукупності даних інформаційної системи.

Приклади непрямих каналів витоку:

- Привласнення чи зникнення засобів зберігання даних: Це може трапитись у формі викрадення чи загублення апаратних компонентів, на яких записана чутлива інформація. Навіть аналіз викинутих відходів може обернутися неочікуваними проблемами.

- Фотографування та аудіозапис із віддаленої відстані: Застосування методів фотографування та прослуховування, здійснюваних на відстані, може слугувати інструментом для отримання закритої інформації без необхідності фізичного наближення.

- Зчитування електромагнітного випромінювання: Застосування визначених апаратур для фіксації електромагнітних сигналів здатне забезпечити доступ до секретних даних без необхідності безпосереднього втручання у функціонування системи.

Приклади прямих каналів витоку:

- Внутрішні протиправні діяння (людський чинник): Злив службової інформації, що трапляється через ігнорування умов щодо комерційної таємниці, може бути спричинений несумлінними кроками найманого персоналу.
- Копіювання безпосереднє: Здійснення фізичного чи електронного тиражування засекречених відомостей може статися завдяки прямому контакту із джерелом їхнього походження.

Поділ каналів зливу відповідно до їхніх фізичних характеристик та принципів роботи охоплює такі групи:

- Візуальні канали: Залучають методи, котрі базуються на зоровому сприйнятті, наприклад, апаратування, запис зображень та моніторинг, для отримання даних.
- Фізичні шляхи: Тут задіяні матеріальні носії відомостей, наприклад, паперові документи або інші субстрати, котрі використовуються для транспортування чутливої інформації.

Розгляд усього спектру шляхів, якими може відбуватися несанкціоноване розповсюдження конфіденційних даних, охоплює як різноманітні підходи, так і потенційні засоби, що можуть бути задіяні зловмисниками для неправомірного доступу до секретних відомостей. Оперативне виявлення подібних інцидентів та вжиття заходів для їхньої нейтралізації перетворюється на ключовий етап у процесі гарантування захищеності інформації.

Окрім того, існує можливість групування цих шляхів витоку інформації з огляду на їхні матеріальні характеристики та базові принципи роботи. Зокрема, інженерно-технічні методи перехоплення розділяються на ті, що виникають спонтанно (природні), та ті, що були цілеспрямовано розроблені (штучні).

Канали для несанкціонованого витоку інформації включають у себе електромагнітні шляхи, які утворюються завдяки побічним електромагнітним випромінюванням, що з'являються під час обробки даних апаратно-програмними комплексами. Додатково, подібні шляхи можуть бути реалізовані через наведення, які проходять по мережах електропостачання, а також через інші електромагнітні явища, здатні призвести до небажаного розголошення

конфіденційної інформації. До власноруч сконструйованих шляхів відносяться пристрої, які мають на меті збір даних, скажімо, усілякі потайні інженерні гаджети.

Їх залучають для формування шляхів несанкціонованого розголошення, інтегруючи електронні компоненти безпосередньо у технічні системи, призначені для роботи з даними. Подібні апарати здатні таємно захоплювати й транслювати інформаційні потоки. Вплив високочастотним випромінюванням на обчислювальні машини тягне за собою генерацію специфічних електромагнітних помутнінь, здатних спровокувати мимовільне випровадження відомостей через радіохвильове випромінювання.

Класифікація шляхів витік даної інформації, зважаючи на її властивості та застосовувані методи, дає змогу глибше осягнути спектр небезпек, з якими може зіткнутися державний апарат. Заходи, спрямовані на нейтралізацію таких каналів, мають брати до уваги усілякі грані та потенціал загроз, аби гарантувати надійний захист конфіденційних відомостей та підтримати інформаційну безпеку як у державних установах, так і серед громадян.

Підсумовуючи огляд загроз інформаційній безпеці, актуальних для державного сектору, слід окреслити декілька фундаментальних моментів. По-перше, необхідно усвідомлювати невпинну трансформацію кіберзагроз, що створює значні труднощі для органів влади. Зловмисники безперервно модифікують свої методики та стратегії, впроваджуючи найновіші технічні засоби та вектори для здійснення атак.

Другим значущим чинником є необхідність запровадження цілісної стратегії кіберзахисту у державному секторі. Йдеться не лише про впровадження технічних бар'єрів, як от охорона мереж і збереження інформації, а й про підвищення кваліфікації персоналу, формування свідомості щодо безпеки та регулярне навчання працівників установ.

Зрештою, третій аспект висвітлює життєву необхідність створення дієвого зв'язку між державними установами, комерційними

співпрацею з вітчизняними установами та союзниками за межами країни у сфері кіберзахисту. Обмін інформацією та узгоджені заходи реагування на кібернетичні загрози здатні відіграти ключову роль у протистоянні кіберагресії та зменшенні її наслідків.

Варто також зосередити зусилля на модернізації механізмів виявлення інцидентів та реагування на них. Створення та впровадження передових інструментів для спостереження й аналізу дасть змогу своєчасно ідентифікувати та нейтралізувати можливі ризики.

Підсумовуючи, забезпечення дієвої кібербезпеки у державному секторі передбачає інтеграцію технологічних рішень, ґрунтовного розуміння кібернетичних небезпек, активної взаємодії та підвищення загальної культури безпеки на всіх рівнях. Тільки застосування такого багатовимірного підходу дозволить гарантувати стійкий захист інформаційних активів та підтримувати високі вимоги до інформаційної безпеки у публічній сфері.

3.2 Концепції та підходи до гарантування інформаційної безпеки під час застосування новітніх інформаційних технологій у сфері державного управління.

Суттєвим елементом, що зумовлює тріумф у царині захисту даних, є готовність до впровадження новацій, зосередження на прогресивних векторах розвитку та висока винахідницька діяльність. Все ширше застосування ІТ-засобів тягне за собою ескалацію загроз у цифровому просторі. Кібератаки спричиняють різнопланові втрати для бізнес-структур. Для подолання цих викликів розроблено значну кількість апаратних і програмних рішень для посилення кібернетичного захисту організацій. Закупівля та створення передових рішень у сфері інфозахисту дає змогу фірмам сформувати дієвий механізм оборони від небезпек, гарантуючи стабільне функціонування та процвітання у перспективі.

На часі, етап розвитку інформаційних технологій вирізняється спроможністю до широкомасштабного впливу інформацією на індивіда та

соціум загалом самосвідомість, часом сягаючи розмаху масштабних інформаційних баталій. У цьому світлі, засада інформаційної захищеності в апараті держави набула статусу життєво важливого контрапункту до доктрини вільного доступу до відомостей. Така трансформація спричинена всеохопною інформаційною епохою, стрімким прогресом та всебічним упровадженням найсучасніших інформаційних засобів та всесвітніх мереж зв'язку.

На основі європейської практики формування інформаційного простору у сфері державного управління для забезпечення сталості розвитку територій, виокремлюється потреба у сталому включенні економічних та соціальних відомостей у процеси управління та комерційної діяльності. З огляду на посилення значущості інформаційного аспекту соціуму, а також наявність технічних та психологічних засобів, що дозволяють впливати на загальну громадську думку, актуалізується потреба у переході до розширеної, прогностичної моделі інформаційного забезпечення. Завданням цієї моделі має бути гарантування адекватного захисту від застосування інформаційних та технологічних технік психологічного тиску, беручи до уваги зростаючий попит суспільства на релевантні дані.

Щодо забезпечення інформаційними ресурсами національної безпеки та збереження приватних даних, неабияке значення має протидія злочинності у кіберпросторі, що є особливо гострою проблемою для держав Європи, які характеризуються значним рівнем впровадження комп'ютерних технологій. Фундаментальним міжнародно-правовим актом, що регламентує суспільні взаємини у сфері протидії кіберзлочинності, слугує Конвенція Ради Європи про кіберзлочин. Переважна частина європейських держав запровадила законодавчі норми, які уможливлюють притягнення до відповідальності суб'єктів господарювання за розміщення протиправного контенту на їхніх веб-ресурсах. Додатково, окремі регуляції накладають обмеження на доступ провайдерів до першоджерел інформації. Хоча оператори мереж не несуть прямої відповідальності за інформацію, що циркулює через їхні мережі, на них покладено зобов'язання вживати належних заходів стосовно тих користувачів та

клієнтів, які застосовують мережі для поширення контенту, що порушує закон. Подібні держави, як-от Об'єднане Королівство, Німеччина та Нідерланди, ухвалили власні збірки правил щодо належної поведінки та заснували незалежні комітети, відповідальні за формування критеріїв етичності контенту й визначення того, що вважати забороненою інформацією.

Аби значно покращити результативність протидії кібертероризму, варто впровадити такий набір кроків:

- Створення ключових державних настанов, доктринальних засад та концептуальних підходів: Впровадження цих основоположних документів у сфері державного керування сталим розвитком певного територіального утворення допоможе кришталево чітко окреслити наміри та конкретні місії стосовно гарантування кіберзахищеності.
- Забезпечення дієвої взаємодії на міжнародній арені: Існує нагальна потреба укладати відповідні домовленості та нарощувати партнерство у сфері обміну відомостями з іншими країнами, їхніми правоохоронними установами та міждержавними структурами. Інтенсифікація такої співпраці стане рушійною силою для обміну напрацюваннями та даними.
- Започаткування оформлення взаємовигідних домовленостей: Підписання подібних пактів розглядається як один із найбільш дієвих механізмів у протистоянні кібернетичним загрозам. Ці домовленості надають можливість консолідувати ресурси задля упередження кібернападів та забезпечення належної відповіді на них.
- Унормування діяльності національного підрозділу протидії кіберзлочинам та міжнародного хабу взаємодії: Запровадження профільних органів сприятиме дієвому впровадженню заходів та профілактиці кіберінцидентів, а також стимулюватиме обмін відомостями й узгодження кроків у світовому масштабі.
- Зобов'язання перед законом та міжнародними нормами: Інкорпорування положень чинного національного законодавства та узгодження

з міжнародними регуляціями, зокрема з Європейською конвенцією про боротьбу з кіберзлочинністю.

- Запровадження законодавства у сфері кібербезпеки: Зважаючи на поточний ландшафт загроз, необхідна відповідна нормативно-правова основа. Ухвалення законів, спрямованих на регулювання електронної безпеки, допоможе сформувати дієві інструменти для протидії кіберзлочинності та актам кібертероризму.

У відповідності до визначеного Плану впровадження Стратегії кібербезпеки України, що був схвалений окремим рішенням Ради національної безпеки та оборони, найпершим завданням для держави постає створення комплексу показників, що відображають рівень кібербезпеки. Цей комплекс передбачатиме наявність основних маркерів стану кібербезпеки, показників прогресу у становленні національної системи кіберзахисту, а також індикаторів рівня захищеності об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та даних, захист яких регламентується законодавством. Ба більше, у цьому Плані також зафіксовано цільові орієнтири, які окреслюють загальну спрямованість усієї Стратегії .

1. Бадьора кіберзахисна система. Наша держава поставить на радування та розбудовування відділків, яким делегують право чинити збройний опір у віртуальному просторі. Окрім того, буде вибудувана відповідна правова, структурна та технічна основа для їхньої роботи і використання. Завдання полягає у тому, аби досягти плідної співпраці між ключовими учасниками загальнодержавної системи захисту від кіберзагроз та військовими формуваннями під час виконання кіберзахисних операцій, а ще – забезпечити належну підготовку та матеріальне підкріплення для таких угруповань. Передбачено регулярне проведення тренувань у сфері кібербезпеки, вивіряння їхніх можливостей та ефективності, а також створення та впровадження показників для судження їхньої роботи. Для досягнення цієї цілі належить здійснити такі кроки:

- Укорінення дієвих порядків співпраці;
- Складання та втілення у життя стратегії із захисту від кіберзагроз;
- -Формування MIL.CERT-UA та налагодження взаємодії з мережею європейських військових CERT.

2. Раціональні заходи супроти вивідувальної та підривної діяльності у віртуальному просторі та кібертероризму. Українська сторона зосередить свої зусилля на підтриманні невпинної реалізації заходів контррозвідувального характеру, спрямованих на викриття, запобігання та зупинку будь-яких спроб розвідувально-підривних дій з боку чужих держав, а також випадків кібершпигунства чи кібертероризму. Головна настанова – ліквідувати передумови, які сприяють появі цих загроз, та усунути їхні першопричини, аби надійно оберігати інтереси країни, громадянства та окремих осіб. Для досягнення цього потрібно запровадити такі кроки:

- Улаштування колективних занять;
- Формування національної мережі забезпечення кібербезпеки;
- Покращення охоронних заходів протидії розвідувальній діяльності у сфері кібербезпеки;
- Підвищення захищеності об'єктів життєво важливої інфраструктури;
- Посилення захисту від контррозвідувальної діяльності у сфері кібербезпеки;
- Створення технічних засобів для розпізнавання кібернетичних нападів;
- Покращення методологій протидії кібертероризму .

3. Дієвий спротив кіберзлочинності. Наша держава ставить собі за мету нарощування спроможностей у межах правоохоронної системи та у визначеному державному органі, наділеному функціями правоохоронної діяльності. Ці спроможності мають бути зосереджені на мінімізації ризиків, що їх створює кіберзлочинність, а також на посиленні як технічного оснащення, так і кваліфікації персоналу. Це забезпечення необхідне для успішного впровадження

профілактичних дій та проведення належного розслідування

інцидентів у кіберпросторі. Для досягнення цього намічено втілення низки кроків:

- Довести до кінця втілення у законодавчу базу України норм, викладених у Європейській конвенції про кіберзлочинність;
- Слід докласти зусиль для врегулювання у встановленій законом процедурі аспектів, що стосуються електронних доказів, при цьому варто спиратися на передові напрацювання, наявні у Сполучених Штатах Америки та країнах Європейського Союзу, а також брати до уваги актуальні проблеми та сучасні вектори розвитку у площині кібербезпеки.;
- Сформулювати концептуальні засади для втілення у життя державної політики стосовно гарантування прав особистостей у кіберсередовищі, зосередивши особливу увагу на найбільш незахищених верствах суспільства, зокрема на неповнолітніх.;
- Впровадити методологію організації загальнодержавної освітньої акції, спрямованої на інформування населення про кроки, яких слід вжити у ситуаціях зіткнення з фішингом чи іншими видами кіберзлочинності, а також деталізувати порядок подання заяв до відповідних правоохоронних структур.;
- Створити методологію для накопичення даних у сфері кібербезпеки та зобов'язати щорічно публікувати статистичні відомості про інциденти, атаки та заходи протидії, згруповані за сферами компетенції ключових учасників національної системи забезпечення кіберзахисту, на їхніх відповідних веб-ресурсах.;
- Створити методологію для здійснення щорічних соціологічних звітів, спрямовану на виявлення кібернетичних ризиків, з якими зіштовхується українське суспільство, а також включатиме оцінку дієвості роботи державних установ у сфері протидії цим загрозам, та забезпечити реалізацію цих досліджень.;
- Сформувати алгоритм взаємодії між владними структурами та

- громадянами стосовно запобігання значним кібератакам та інцидентам у кіберпросторі, а також забезпечити практичну реалізацію цього алгоритму шляхом створення відповідних передумов;

- Слід упровадити процедури верифікації учасників інтернет-торгівлі у мережі, для чого необхідно внести корективи у чинне законодавство України;;

- Унормувати у визначений спосіб правовий стан (статус) криптоактивів.;

- Організовувати спільні із Європейським Союзом та НАТО події, мета яких - посилення захисту від кібернетичних загроз та нарощування потенціалу для розслідування, притягнення до відповідальності за кіберзлочини і відповідного реагування на кібернетичні виклики.;

- Потрібно здійснити заходи для покращення майстерності судових експертів, а також оновлення їхньої матеріально-технічної бази, зокрема у сферах експертизи комп'ютерної техніки, програмного забезпечення, а також комунікаційних систем і засобів.;

- Потреба у підвищенні обізнаності персоналу оперативних служб, слідчих органів, прокуратури та судового корпусу у сфері інфотехнологій та кібернетичного захисту є нагальною, особливо ж стосовно методик вилучення й аналізу цифрових доказових матеріалів.;

- Залучення приватних фахівців для здійснення комп'ютерно-технічних та телекомунікаційних аналізів, а також експертиз програмного забезпечення, які обумовлені потребою оперативного реагування на кіберподії та результативного розкриття кіберзлочинів.

2. Вдосконалення асиметричних засобів стримування. З метою гарантування стримування ворожих діянь у кіберпросторі, спрямованих проти нашої держави, Україна створюватиме відповідну інфраструктуру, залучаючи до цього як економічні, дипломатичні та розвідувальні ресурси, так і можливості приватного бізнесу. З огляду на значний рівень небезпеки, що виходить із цієї сфери, Україна рішуче підтримуватиме підвищення рівня

кіберзахисту через налагоджену та плідну співпрацю з усіма верствами суспільства та нашими міжнародними союзниками.

3. Кіберстійкість на рівні держави та забезпечення непорушного захисту у кіберпросторі. З метою забезпечення процвітання економіки та охорони прав і вольностей кожного українця, наша держава впровадить чіткі, прозорі для усіх причетних кроки у сфері національної кіберготовності. Рівень боєздатності у кіберпросторі буде підвищено, з акцентом на спроможність усіх задіяних суб'єктів, особливо у секторі безпеки та оборони, оперативно і результативно протистояти кібератакам. Це вимагає гарантування постійної готовності до актуальних та можливих кіберризиків, унеможливлення умов для їх виникнення, а також нарощування кіберстійкості, насамперед об'єктів, що входять до критичної інформаційної інфраструктури.

Ба більше, Україною буде розгорнуто загальнодержавну систему для управління інцидентами, що забезпечить злагодженість і результативність у врегулюванні кіберінцидентів. Усі ці дії мають на меті посилення кіберзахисту держави, мотивоване прагненням досягти найвищого ступеня захищеності від загроз у кіберсфері для гарантування стабільності та безпеки України у цифровому вимірі .

Професійне вдосконалення, кіберобізнане суспільство та науково- технічне забезпечення кібербезпеки.

4. Посилення механізмів узгодженої діяльності. Україна рішуче налаштована на підтримку злагодженої роботи усіх учасників процесу забезпечення кібербезпеки під час формування та функціонування вітчизняної системи кіберзахисту. Держава створить сприятливе підґрунтя для плідної взаємодії та спільних кроків у напрямку запобігання, протидії та мінімізації наслідків кібератак та інцидентів у цифровій сфері. У конкретному вимірі, буде організовано узгодження дій усіх причетних сторін для виходу з надзвичайних (кризових) обставин у кіберпросторі. Ця програма на увазі запровадження

дієвих інструментів партнерства та обміну відомостями між різноманітними ланками кібербезпеки, а саме: урядовими структурами, комерційним сектором та громадськими організаціями. Українська сторона усі свої потуги фокусує на формуванні прозорого та працездатного формату взаємодії, що дасть змогу результативно реагувати на виклики в кіберсфері та координувати спільні дії задля гарантування кіберзахисту держави.

5. Створення оновленого шаблону взаємодії у царині кібербезпекових питань. Наша держава опановує сервісний підхід до ролі уряду щодо кіберзахисту, де влада постає не лише як орган, що встановлює критерії, а як дієвий співучасник у розбудові вітчизняної системи стійкості до кіберзагроз. Така новаторська парадигма наголошує на необхідності налагодження партнерських зв'язків поміж державними інституціями, приватним капіталом та громадськими об'єднаннями задля колективного гарантування належного обороту кіберпростором держави.

6. Практична міжнародна взаємодія. Україна будує контакти з країнами-партнерами не лише на засадах взаємної довіри задля спільної протидії кібернападам та виходу з кризових станів у сфері кіберзахисту, а й на засадах активної роботи на землі. До цього залучається надання даних про здійснені кібератаки та інциденти, проведення спільних операцій у кіберсфері та розслідування кіберзлочинів, що мають транскордонний характер, регулярне проведення спільних кібертренувань та навчань, а також обмін набутками та найбільш ефективними методиками. Наша держава гарантуватиме свою активну присутність у дискусіях у межах міжнародних інституцій з метою спільного формування правил поведінки у віртуальному просторі та покращення існуючої законодавчої бази. Узгодження дій з міжнародними партнерами покладатиметься на Міністерство закордонних справ України.

Практична міжнародна взаємодія. Україна будує контакти з країнами-партнерами не лише на засадах взаємної довіри задля спільної протидії кібернападам та виходу з кризових станів у сфері кіберзахисту, а й на засадах активної роботи на землі. До цього залучається надання даних про здійснені

кібератаки та інциденти, проведення спільних операцій у кіберсфері та розслідування кіберзлочинів, що мають транскордонний характер, регулярне проведення спільних кібертренувань та навчань, а також обмін набутками та найбільш ефективними методиками. Наша держава гарантуватиме свою активну присутність у дискусіях у межах міжнародних інституцій з метою спільного формування правил поведінки у віртуальному просторі та покращення існуючої законодавчої бази. Узгодження дій з міжнародними партнерами покладатиметься на Міністерство закордонних справ України.

Отримання належного рівня інформаційної безпеки вимагає залучення передових технологічних рішень, утвердження чітких нормативів та створення дієвих протоколів кіберзахисту. В основі цього процесу лежить обов'язковий аналіз потенційних кібернетичних загроз та оперативне реагування на них, гарантування збереження та незмінності даних, а також підтримання їхньої доступності. Крім того, критично важливим є вдосконалення механізмів координації між управлінськими ланками для спроможності оперативно реагувати на можливі надзвичайні обставини.

Впровадження дієвих засад інформаційної безпеки у сфері державного управління вимагає поєднання новітніх практик, підготовки кадрів, а також формування оперативних систем для ідентифікації та реагування на випадки порушення безпеки. Установам публічної влади необхідно налагоджувати тісну взаємодію із сектором приватного бізнесу та залучати проривні технології, аби гарантувати комплексний та надійний захист даних.

Зважаючи на викладене, слід визнати, що першочерговим і найважливішим етапом є імплементація усіх окреслених ідей та чинних регуляцій безпосередньо у структуру владних інституцій. Насамперед, це стосується апарату державних органів, відповідальних за публічне управління, зокрема, йдеться про районні та міські ради, а також виконавчі структури, підпорядковані міським головам. Планована комплексна схема забезпечення інформаційної надійності має охоплювати широкий спектр функцій та дій, спрямованих на захист і збереження

конфіденційності, цілісності та належної доступності інформаційних ресурсів у межах встановленої системи чи платформи.

Узгодження стратегії захисту інформації на підприємстві, у відомстві чи об'єднанні - це не якийсь одноразовий захід. Гарантування інформаційної безпеки являє собою колосальний діловий процес, якщо розглядати його з погляду політики, технології та адміністрування. Він тією чи іншою мірою вимагає прийняття численних рішень керівництвом, а також значних аналітичних навичок та освіченості у сфері інформації.

Гора інформаційної безпеки нормативів, створених різноманітними світовими й вітчизняними установами, має місце:

- ISO/IEC 27001: Тут окреслено критерії, яким має відповідати система керування інформаційною безпекою (СКІБ), а також запропоновано універсальну методологію управління впровадженими заходами у сфері інформаційної безпеки.
- ISO/IEC 27002: Цей стандарт охоплює детальні настанови з імплементації заходів контролю, які перелічені у ISO/IEC 27001.
- NIST SP 800-53: Американський Національний Інститут Стандартів і Технологій (NIST) створив цей документ, що містить перелік заходів контролю для інформаційних систем та установ федерального рівня.
- COBIT (Control Objectives for Information and Related Technologies): Методологічна основа (фреймворк) для нагляду та керування інформаційними технологіями у межах установи.

PCI DSS (Payment Card Industry Data Security Standard): Встановлює критерії щодо збереження таємності комерційної інформації, що стосується платіжних карток.

Ці нормативи окреслюють необхідні приписи та пропозиції, які сприяють установам будувати дієві механізми контролю за інформаційною безпекою та гарантувати належний ступінь оберігання даних.

Здійснений розгляд як теоретичних положень, так і практичних

відомостей, викладених у попередніх частинах, надав нам можливість сформулювати та представити один із можливих зразків послідовності дій для гарантування захищеності інформації у межах апаратів та структур органів державної влади.

Перша фаза цієї запропонованої послідовності передбачає офіційне схвалення (узаконення) у межах установи плану дій щодо забезпечення інформаційної безпеки. Процедура створення та впровадження такого плану для будь-якої організації чи установи охоплює низку кроків: від початкових організаційних заходів до подальшого контролю та внесення коректив після того, як його було прийнято.

Ось загальний цикл:

1. Попередній аналіз та визначення потреб:

- З'ясування поточного стану: Детальне дослідження обставин інформаційної безпеки, ідентифікація вже наявних загроз та слабких місць.
- Визначення цілей та меж: Складання чітких намірів та завдань для стратегічного плану.

2. Збирання та опрацювання вихідної інформації:

- Залучення стейкхолдерів: Залучаючи головних учасників та зацікавлені сторони задля збору широкого спектру поглядів.
- Збирання відомостей: Опрацювання та ретельне вивчення даних стосовно наявних угруповань, послідовностей дій та потенційних небезпек.

3. Розробка стратегії:

- Установлення заходів безпеки: Створення головних засад та норм для охороняння відомостей.
- З’ясування кроків для кібербезпеки: Уточнення, які саме методи та технологічні рішення будуть застосовані з метою превенції та ідентифікації загроз у кіберпросторі.

4. Затвердження та впровадження:

- Впровадження заходів: Розпочаток реалізації запланованих заходів та політик.

Ось цей ланцюжок подій має циклічний характер, тож установі мусить невпинно шліфувати свій підхід, реагуючи на мутації в сфері кібернетичних загроз, технологічні прориви та власні потреби.

Як тільки Політику інформаційної безпеки офіційно схвалено, установа переходить до етапу втілення та практичного виконання цієї стратегії. На цій стадії ключовими кроками є:

- Розгортання стратегії: Формування плану розгортання стратегії, включаючи визначення відповідальних за виконання завдань та терміни їх виконання.
- Формування бізнес-стратегії: Необхідно виробити чіткий план дій, який окреслюватиме розподіл обов'язків, фінансове забезпечення, часові рамки реалізації та показники, за якими буде оцінено досягнення мети.
- Формування й запровадження регламентів та правил: Розробка таких правил та інструкцій з інфобезпеки, що узгоджуються з визначеними цілями та напрямками стратегічного плану.
- Підготовка кадрів та їх включення до процесу: Організація тренінгів та інструктажів для співробітників щодо аспектів кіберзахисту, особливо в контексті оновлених регламентів та встановлених порядків.
- Запровадження інженерних рішень: Здійснення тих технічних кроків, що були окреслені у стратегії, наприклад, інсталяція свіжих комплексів для охорони, спостереження та збереження даних.

1. Третя стадія у звичному проєкті, так само, охоплює загальні аспекти й не має жодних часових обмежень. Безумовно, після того, як Стратегію захисту даних запроваджено та необхідні кроки виконано, увесь цикл здатний розпочатися знову, або ж установа має можливість не припиняти підтримання та модернізацію своїх заходів кіберзахисту відповідно до нових загроз і технологічного розвитку. До цього, природно, увійдуть наступні безперервні

дії::

2. Нагляд та інспектування: Невпинне простежування даних, одержаних із заздалегідь розгорнутих систем спостереження, а також здійснення періодичних перевірок з метою з'ясування дієвості запроваджених заходів і за потреби реагування на виникаючі небезпеки.

3. Неперервне Покращення: Запровадження механізмів невпинної оптимізації системи захисту інформації, беручи до уваги еволюцію технологій, а також внутрішні та зовнішні ризики.

4. Інформування та Доповіді: Систематичне представлення відомостей щодо стану захисту інформації вищому керівництву та усім причетним суб'єктам.

5. Відповідь на події: Створення та залучення до виконання плану реагування на інциденти, що дозволить оперативно та дієво реагувати на будь-які випадки порушення безпеки інформації..

Висновки за розділом 3

З’ясовано, що державний сектор оперує у середовищі, де він піддається численним небезпекам та потенційним втратам у сфері інформаційної безпеки, що зумовлено стрімким упровадженням новітніх технологій. До переліку цих загроз належать, зокрема, кібернетичні нападки, несанкціоноване розголошення конфіденційної інформації та інші актуальні виклики сьогодення.

Ключовим складником дієвого щита є формування та реалізація відповідних підходів до забезпечення інформаційної безпеки. Нинішні ІТ-плани мусять охоплювати багатовекторні кроки, націлені на превентивні дії, ідентифікацію та нейтралізацію загроз, що стосуються інформації.

Досліджені стратегії інформаційної безпеки в середовищі органів публічного управління відповідно до міжнародних стандартів. Зазначено, що вироблення та впровадження стратегій повинно відповідати визначеним

стандартам та нормативам для забезпечення високого рівня безпеки.

У цьому розділі підсумовано, що задля дієвого гарантування інформаційної безпеки потрібна єдність технічних та управлінських кроків. Недостатньо, щоб компанії лише впроваджували передові технології; їм також необхідно запровадити дієві регламенти та усталені норми захисту.

Слід усвідомити, що активне застосування ІТ-засобів обумовлює необхідність незмінного контролю та ревізії підходів до захисту інформації. Оскільки загрози еволюціонують, критично значущо адаптувати запроваджені превентивні заходи відповідно до мінливих реалій. Базуючись на даних, викладених у цьому дослідженні, було сформовано стандартний алгоритм гарантування інформаційної безпеки саме в межах системи органів державної влади. Він охоплює три ключові фази: починаючи із початкового етапу планування та формування стратегії захисту, продовжуючи фактичним впровадженням регламентів та апаратних/програмних рішень, і завершуючись постійним супроводом та наглядом.

Даний розділ окреслює головні стратегічні напрямки, необхідні для гарантування дієвої захищеності інформації при активному впровадженні новітніх ІТ-рішень у сфері державних послуг, акцентуючи увагу на незамінності системного бачення.

ВИСНОВКИ

Роблячи загальний висновок, слушно буде зазначити: у нинішню еру інформаційних технологій відбувається докорінна перебудова усіх аспектів суспільного буття, що, безперечно, стосується і сфери державного урядування. Посилення комп'ютеризації та впровадження автоматизованих рішень у процеси, що стосуються роботи органів влади, створюють значні труднощі й вимагають всебічного усвідомлення того, як саме інфокомунікаційні засоби позначаються на продуктивності та захищеності управлінських методик.

Дослідження можливостей, які надають інформаційні технології, виявило їхню здатність слугувати потужним важелем для вдосконалення механізмів публічного адміністрування. Запровадження електронних урядових платформ дає змогу автоматизувати чимало функціональних задач держструктур, гарантуючи швидку й якісну реалізацію доступу громадян до необхідних сервісів.

Інформаційні технології зайняли центральне місце у модернізації роботи урядів та покращенні обслуговування населення, надаючи свіжі перспективи для зростання результативності та прозорості державного управління. Водночас, інновації є невід'ємною складовою сучасного соціуму, диктуючи напрямок його майбутнього поступу та добробуту. Сутність інновацій полягає у запровадженні передових концепцій, апаратних рішень, товарів та способів ведення справ у найрізноманітніших сферах буття.

Останні інноваційні розробки, зокрема концепція "розумних міст" та застосування технологій Інтернету речей, сприяють раціоналізації керування енергетичними ресурсами та транспортними потоками. Системи електронної медицини та цифрові освітні платформи спрощують отримання доступу до послуг у сферах охорони здоров'я та навчання. Фінтех, платформи соціальних комунікацій та електронна демократія відкривають перед нами нові можливості для підвищення дієвості та залучення громадян до механізмів правління, посилюючи тим самим конкурентні переваги суспільства.

Електронні та комунікаційні засоби у державній адміністрації приносять користь, оскільки вони надають:

- Гарний доступ до відомостей.
- Оптимальне розпорядження часом та засобами.
- Вільний дозвіл на користування державними сервісами.

Ці чинники реалізуються завдяки інноваційному менеджменту, який є системою керування, що має на меті формування середовища для процвітання та успішного застосування нововведень у межах підприємства.

У цьому дослідженні окреслені найсучасніші напрями та технічні прориви у сфері державного управління, що охоплюють такі складові:

- Електронна урядова діяльність (е-Уряд).
- Дистанційна освіта
- Системи керування проєктами в цифровій формі і тому подібне.

У цьому контексті було представлено до уваги перелік зразків українських та іноземних розробок, які ілюструють усі напрями застосування технологічних новацій у сфері адміністрування, як на рівні держави, так і на рівні територіальних громад. З огляду на це, встановлено, що інтеграція найсучасніших технологій у сферу державного управління має на меті підвищення добробуту населення та досягнення результативності роботи органів влади.

У другій частині цього дослідження зосереджено увагу на електронних урядових системах, які є ключовим складником інформаційних технологій у сфері державного управління.

Тут розкриваються еволюційні етапи розвитку електронного урядування, що поділяється на дві окремі фази.

Крім того розглянуті моделі реалізації систем електронного урядування, а саме:

- Централізована модель.
- Децентралізована модель.

Окрім цього, у наявності є певна кількість індикаторів та зразків стратегічних підходів, рівно як і доповнювальні практичні зразки для вимірювання розвитку електронного урядування. Усі ці розроблені моделі та індекси охоплюють багатоступеневі процеси. Ключовою є концепція поступового просування від однієї стадії до наступної, де кожна подальша фаза передбачає удосконалення та збільшення доступного функціоналу.

Окрім того, наявна зведена таблиця типових труднощів та перешкод, виявлених у процесі аналізу літератури. Ці чинники здатні уповільнити експансію електронного урядування під час його запровадження. Це дає нам підстави констатувати, що запуск електронного уряду - це нетривіальне доручення, яке неминуче наштовхується на низку складнощів та перепон, що потребують ретельного дослідження й успішного подолання.

Під час аналізу законодавчих актів було встановлено, що у сфері публічного та державного управління система функціонує з метою досягнення таких завдань:

- Формування спільного сховища інформації стосовно державних службовців та персоналу уповноважених органів.
- Механізація й переведення у цифровий формат процесів, пов'язаних із керуванням персоналом та ухваленням рішень щодо особового складу.
- Нагляд за ефективністю роботи у підрозділах, що залучені до кадрового адміністрування.
- Гарантування відкритості та зрозумілості відомостей стосовно особового складу та винагороди за працю.
- Зміцнення потенціалу відділів, що займаються кадровим забезпеченням та фінансовою звітністю.
- Еволюція нинішнього менеджменту людських активів завдяки швидкості і достовірності реєстрації даних.
- Діяльність інформаційних систем у сфері державного управління та електронний обмін даними.

Окреслені цільові установки насправді слугують головними орієнтирами, які окреслюють значення інфокомунікаційних систем у процесі вдосконалення державного управління.

Загалом, можна констатувати, що цифрові технології закладають основу для переосмислення управлінських парадигм у сфері публічного адміністрування, акцентуючи їхню ключову роль у досягненні високої продуктивності та зміцненні зв'язку між державними інституціями та населенням.

Вимога щодо надійного забезпечення інформаційної безпеки зумовлена не лише внутрішніми потребами державних структур, а й їхніми зобов'язаннями перед суспільством. Збереження конфіденційності даних є однією з фундаментальних задач органів влади, оскільки їхній провал може спричинити технічні збої та підірвати довіру громадськості, що, своєю чергою, негативно позначиться на легітимності та спроможності управлінських структур.

На підставі ретельно проаналізованих відомостей, отриманих із різноманітних джерел, окреслено ключові небезпеки, що стосуються інформаційної безпеки у сфері державного управління:

- Напади в цифровій сфері, а також кримінальна діяльність у мережі у широкому сенсі;
- Розголошення таємних відомостей.

У цьому ж дослідженні окреслено ключові проблеми у сфері інформаційної безпеки, що постали внаслідок бойових дій. З метою забезпечення комплексного розуміння, наведено орієнтовний перелік шляхів несанкціонованого розголошення даних, куди входять як безпосередні, так і опосередковані методи.

Якщо конфіденційні відомості потраплять до третіх осіб, це може спричинити для державних інституцій та громадян такі наслідки: зниження рівня довіри до органів влади, зростання імовірності корупційних проявів, небезпеку для обороноздатності країни, і, як наслідок, потенційну втрату

конкурентних переваг державних структур на економічному фронті.

У фінальному розділі здійснили розгляд значного обсягу міжнародних норм стосовно безпеки інформації. Спираючись на накопичені відомості та вивчені у праці першоджерела, було вироблено пропозиції щодо зразкової послідовності дій для гарантування інформаційної безпеки у підрозділах та апаратах державних органів.

Ця послідовність складається з таких кроків::

- Початковий етап, що охоплює з'ясування обставин та встановлення вимог, складається з таких кроків: розгляд поточної обстановки, конкретизація цілі та меж роботи, накопичення й дослідження вхідної інформації, залучення усіх причетних осіб, а також опрацювання здобутих відомостей.
- Ключові кроки у цьому процесі охоплюють формування стратегічного бачення, формування бізнес-плану, вироблення та запуск у дію регламентів і порядків, проведення тренінгів та активізацію співробітників, а також впровадження технологічних рішень.

Після того, як План інформаційної безпеки введено в дію та необхідні кроки виконано, цей цикл має потенціал для повторення. Альтернативно, установа може перейти до етапу підтримання й оновлення своїх заходів захисту інформації, реагуючи на нові загрози та технологічний прогрес.

Серед постійних дій у цьому контексті будуть:

- Нагляд та ревізія, куди входять механізми спостереження й інспектування, з метою визначення дієвості вжитих кроків та заходів реагування на потенційні небезпеки.
- Невпинна оптимізація системи захисту інформації, беручи до уваги як технологічні інновації, так і наявні загрози.
- Постійне інформування вищого керівництва та зацікавлених сторін щодо рівня інформаційної безпеки.
- У відповідь на події, шляхом створення та запровадження певного плану.

Підсумовуючи результати виконаного аналізу, варто наголосити: використання інформаційних технологій у сфері державного управління суттєво спрощує функціонування владних структур, зумовлює пришвидшення процесу надання сервісів та гарантує дієвий обмін даними. Водночас, інтеграція цих технологій породжує і новітні проблеми у сфері інформаційної безпеки, що диктує необхідність безперервного вдосконалення підходів та впровадження заходів задля охороні чутливої інформації від усього спектру потенційних небезпек. Баланс між перевагами ІТ та вимогами до надійності кіберзабезпечення набуває ключового значення у контексті управління державними справами сьогодення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Castells, M. *The Rise of the Network Society*. Oxford: Blackwell, 2010.
2. West, D. Digital Government: Technology and Public Sector Performance. Brookings Institution Press, 2017.
3. Janssen, M., et al. “Benefits, Adoption Barriers and Myths of Open Data.” Information Systems Management, 2012.
4. Bertot, J.C., Jaeger, P.T. “Transparency and Open Government in the Digital Age.” Government Information Quarterly, 2010.
5. Nam, T. “Smart City Design Factors: ICT Challenges.” Government Studies Journal, 2018
6. Andersen, K. V., Henriksen, H.Z. “Digital Governance and Public Sector Innovation.” Information Polity, 2017.
7. Margetts, H. Public Policy in the Digital Era. Oxford University Press, 2019.
8. European Commission. Digital Public Services Report, 2023.
9. Singh, A., Sharma, S. “Artificial Intelligence in Public Administration.” AI & Society, 2020.
10. Brown, D. “E-government and Public Administration Modernization.” Public Management Review, 2015.
11. United Nations. E-Government Survey, 2022.
12. OECD. Digital Government Index, 2021.
13. Lee, J. “Blockchain Adoption in the Public Sector.” Technology Forecasting and Social Change, 2021.
14. Scholl, H.J. “E-Government Integration Challenges.” Digital Government Research Conference Proceedings, 2019.
15. Pavlenko, O. “Digital Transformation of Ukrainian Public Services.” Ukrainian Journal of Public Policy, 2022.
16. Kshetri, N. “1 Big Data Applications in the Public Sector.” International Journal of Public Information Systems, 2018.

17. Meijer, A. “Understanding the Digital Transformation of Government.” Public Management Review, 2019.
18. Singh, A. “Data Governance in E-Government Systems.” Government Information Quarterly, 2019.
19. Колос О., Каленська К. Еволюція розділу xvi кримінального кодексу україни в умовах імплементації положень конвенції ради європи про кіберзлочинність. Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки. 2022. Т. 60, № 1. С. 11–17. URL: https://doi.org/10.32689/2522-4603.2021.1.2 (дата звернення: 10.10.2023).
20. Юдкова К. В. Особливості визначення поняття "інформаційна система”. Інформація і право. 2015. № 2 (14). С. 39–44.
21. Greenleaf, G. “Privacy Laws in Public Administration.” International Data Privacy Law, 2018.
22. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 11.09.2023).
23. Zhao, Y. “AI-Driven Decision Making in Government.” Computers in Human Behavior, 2020.
24. Звіт Мінцифри. Розвиток екосистеми «Дія». Київ, 2023
25. Верховна Рада України. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
26. Марущак А. “Електронна демократія в Україні.” Державне управління та місцеве самоврядування, №3, 2021.
27. Литвиненко О. “Сучасні виклики кібербезпеки в Україні.” Кібербезпека: освіта, наука, техніка, 2022.
28. Національний банк України. Кіберзахист фінансового сектору України: аналітичний звіт 2023.

29. Державна служба спеціального зв’язку та захисту інформації України. Щорічна доповідь про стан кібербезпеки. Київ, 2022.
30. Верховна Рада України. Закон України «Про електронні довірчі послуги». № 2155-VIII від 05.10.2017.
31. Баранов О. “Цифровізація публічних послуг в Україні.” Вісник НТУУ «КПІ». Соціологія. Політологія., 2021.
32. Український союз промисловців та підприємців. Цифрова трансформація бізнесу і держави, 2021.
33. Державна служба спеціального зв’язку та захисту інформації України. Щорічна доповідь про стан кібербезпеки. Київ, 2022.
34. Аналітичний центр «Український інститут майбутнього». Ukraine GovTech Review 2023
35. Дубов Д. Кібербезпека в Україні: виклики та загрози. К.: НІСД, 2020.
36. Державна служба спеціального зв’язку та захисту інформації України. Щорічна доповідь про стан кібербезпеки. Київ, 2022.
37. Greenleaf, G. “Privacy Laws in Public Administration.” International Data Privacy Law, 2018.
38. Харківський національний університет радіоелектроніки. Збірник праць з кібербезпеки №4, 2022.
39. Баранов О. “Цифровізація публічних послуг в Україні.” Вісник НТУУ «КПІ». Соціологія. Політологія., 2021.
40. Сорока Л. “Електронне урядування в Україні: реалії та перспективи.” Державне управління: теорія та практика, №1, 2020.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ГАЛУЗІ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ ТА ЇХ ВПЛИВ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ»

на здобуття освітнього ступеня маігстра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав: Терещенко Д.С, ІСДМ-61

Науковий керівник роботи:

Данильченко В.М.

Київ - 2025

Актуальність дослідження

Цифрова трансформація публічного адміністрування є ключовим напрямом розвитку держави.

Щорічно збільшується кількість електронних сервісів та інформаційних систем.

Зростає обсяг персональних даних, що обробляються органами влади.

Порушення інформаційної безпеки призводять до значних соціальних та репутаційних втрат.

Забезпечення інформаційної безпеки є необхідною умовою ефективної цифровізації.

Мета роботи – дослідити вплив інформаційних технологій на систему публічного адміністрування.

Завдання дослідження:

Проаналізувати сучасні напрями цифровізації органів публічної влади.

Визначити основні загрози інформаційній безпеці цифрових сервісів.

Оцінити рівень інформаційних ризиків на основі аналітичного підходу.

Об’єкт і предмет дослідження

Об’єкт дослідження – система публічного адміністрування як сукупність управлінських процесів.

Предмет дослідження – інформаційні технології та механізми захисту інформації.

Фокус дослідження зроблено на електронних сервісах та цифрових платформах.

Динаміка цифровізації публічного адміністрування

Лінійний графік демонструє сталу тенденцію до зростання цифровізації у 2019–2024 роках.

Найбільш інтенсивне зростання спостерігається після масового впровадження електронних послуг.

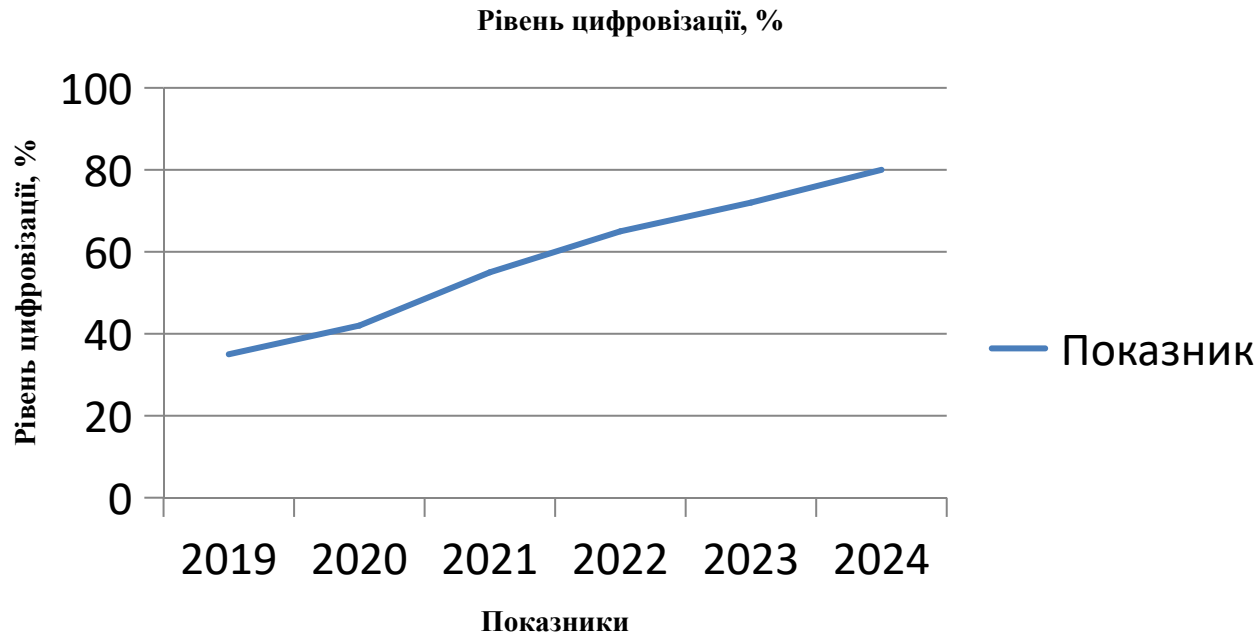

Рисунок: 4.1 Лінійний графік

Стовпчикова діаграма відображає щорічне зростання кількості інцидентів витоку даних.

Збільшення кількості цифрових сервісів призводить до розширення поверхні атак.

Рисунок: 5.1 Стовпчикова діаграма

Лінійний графік демонструє зростання масштабу негативних наслідків витоку інформації.
Отримані дані свідчать про необхідність посилення заходів інформаційної безпеки.

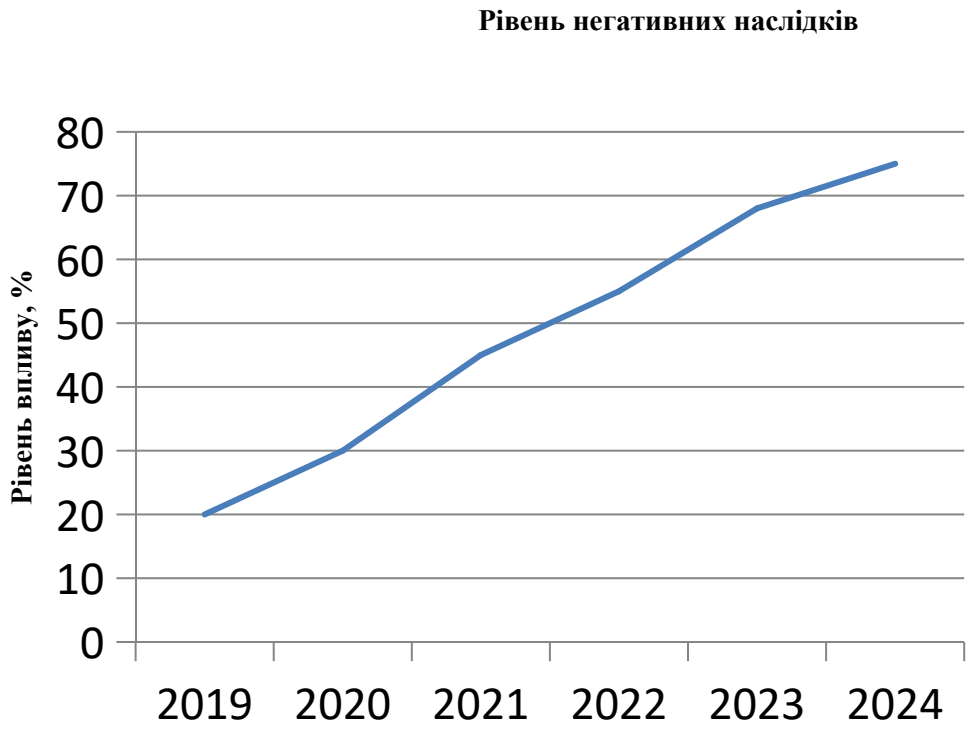

Рисунок: 6.1 Лінійний графік

Кругова діаграма демонструє співвідношення основних типів загроз інформаційній безпеці.

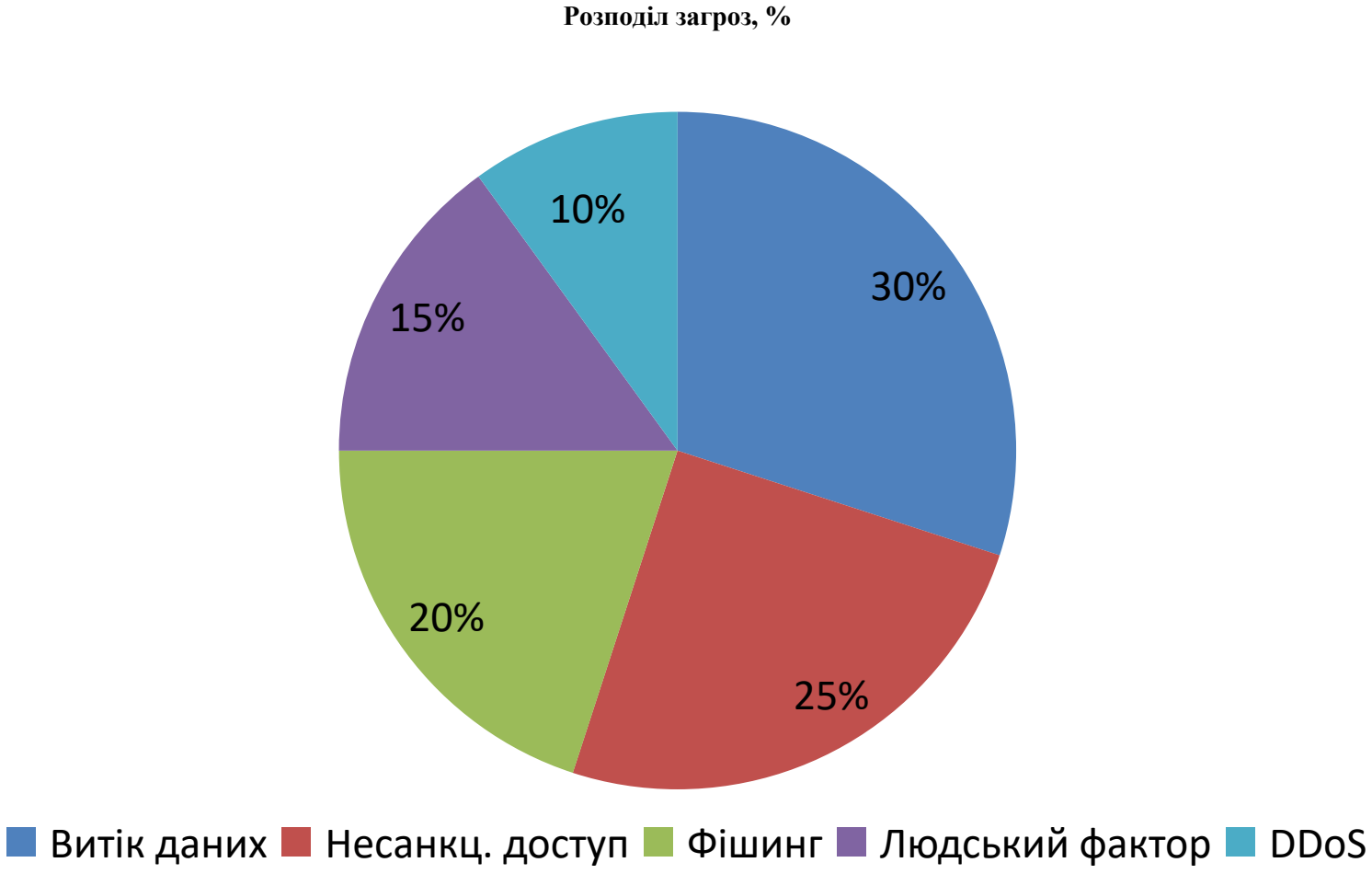

Рисунок:7.1 Кругова діаграма

Оцінка рівня інформаційних ризиків

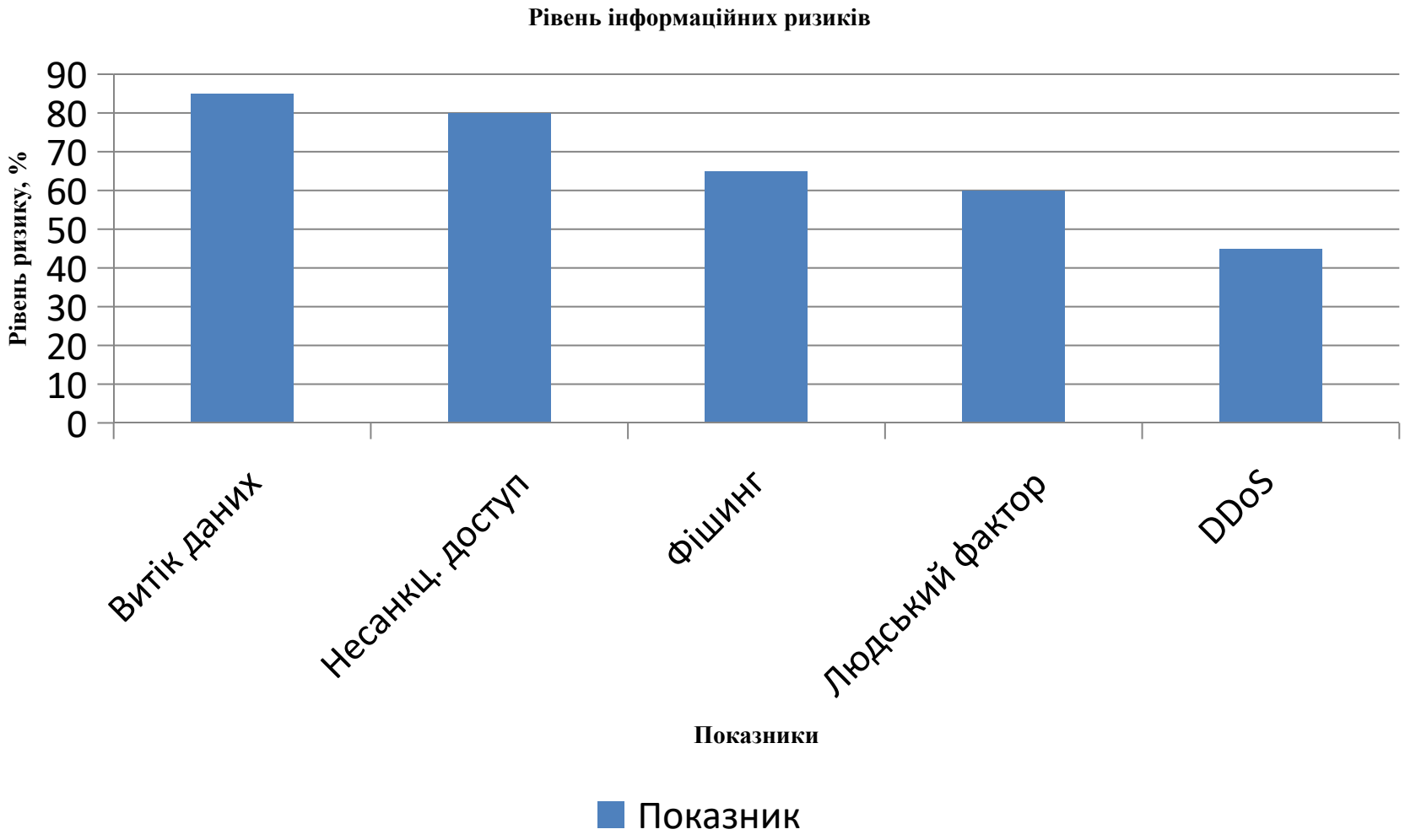

Рисунок: 8.1 Стовпчикова діаграма

Вплив заходів безпеки на рівень ризиків

Лінійний графік демонструє зміну інтегрального рівня ризику до та після впровадження заходів.

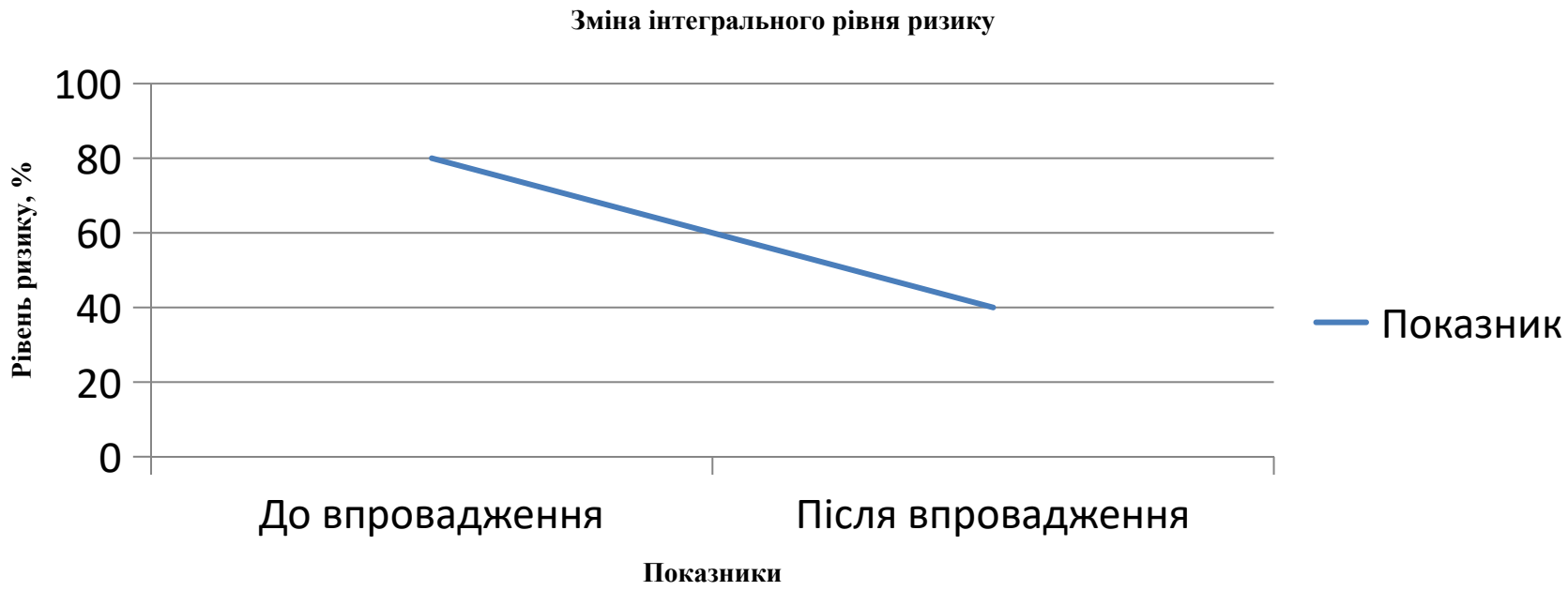

Рисунок: 9.1 Лінійний графік

Запропоновані заходи підвищення інформаційної безпеки

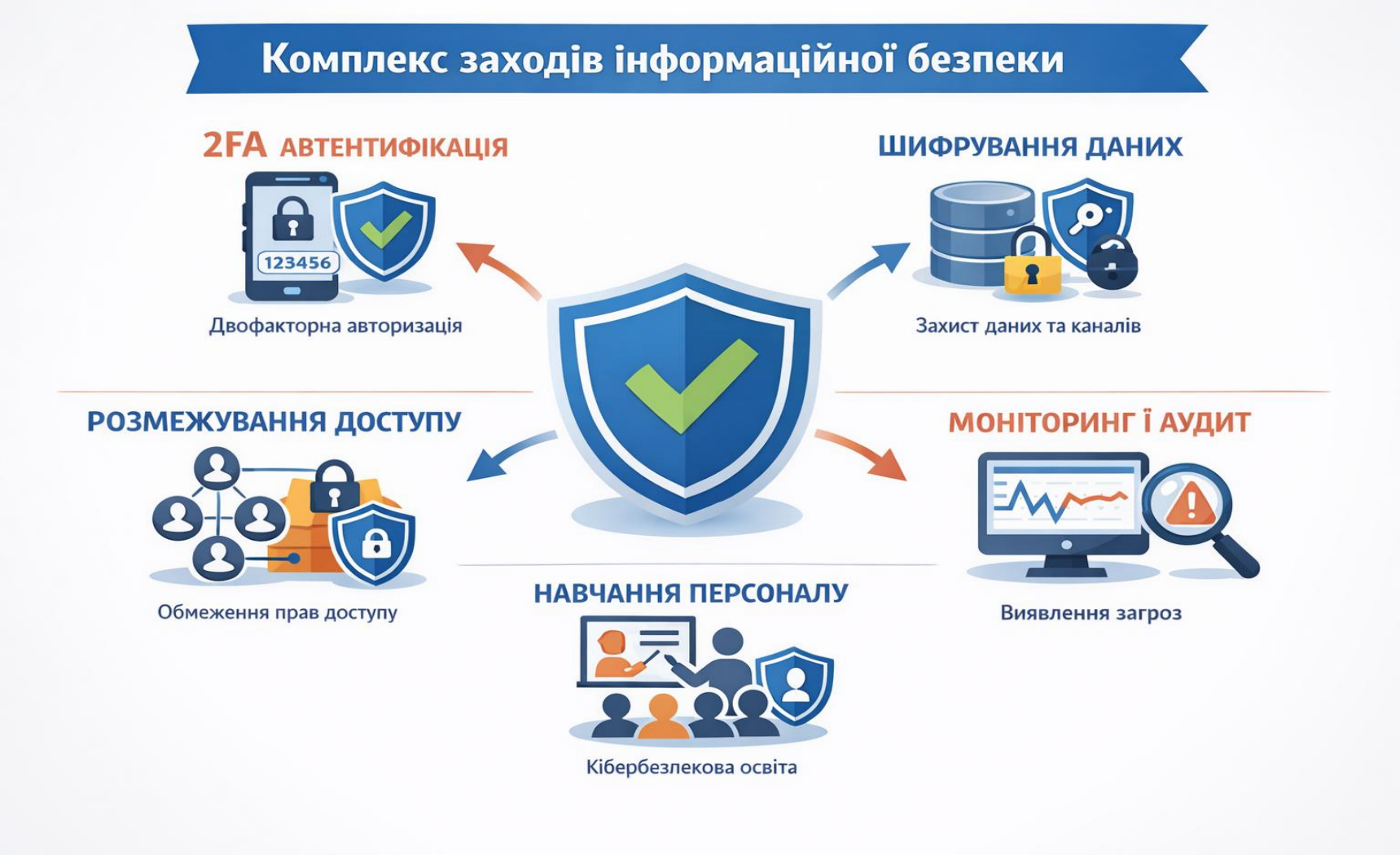

Рисунок: 10.1 Приклад заходів

Висновки

1. Цифровізація публічного адміністрування демонструє стійку позитивну динаміку, що підтверджується зростанням рівня використання інформаційних технологій у 2019–2024 роках.

2. Розширення цифрових сервісів супроводжується збільшенням кількості та масштабу інцидентів витоку інформації, що підвищує рівень інформаційних ризиків.

3. Найбільш критичними загрозами інформаційній безпеці є витік персональних даних (30%) та несанкціонований доступ (25%), що потребує першочергових заходів захисту.

4. Проведена оцінка ризиків засвідчила високий рівень небезпеки для ключових цифрових сервісів публічного адміністрування.

5. Запропоновані технічні та організаційні заходи дозволяють знизити інтегральний рівень ризиків приблизно вдвічі.

6. Мету та завдання магістерської роботи виконано в повному обсязі, отримані результати мають практичне значення.

7. Результати дослідження можуть бути використані в органах публічної влади.

8. Запропонований підхід дозволяє оцінювати рівень інформаційних ризиків.

9. Матеріали роботи можуть застосовуватись у навчальному процесі.

10.Рекомендації сприятимуть підвищенню рівня захисту електронних сервісів.

Апробація

1. Всеукраїнська наукова конференція: ”Актуальні проблем кібербезки” на тему “Кібербезпека корпоративних інформаційних систем” ст.208 24 жовтня 2025 року.

2. ІІ Всеукраїнській науково-технічній конференції “Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу” на тему “ Технологічні інновації в освіті ”

Дякую за увагу!