

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ЦЕНТР ПІДГОТОВКИ МАГІСТРІВ ПУБЛІЧНОЇ СЛУЖБИ
І ПРОФЕСІЙНИХ СУДДІВ
Кафедра психології

МАГІСТЕРСЬКА РОБОТА

на тему:

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

Виконала: здобувачка вищої освіти 2 курсу
заочної форми навчання, галузі знань 28
«Публічне управління та адміністрування»
спеціальність 281 «Публічне управління та
адміністрування»

Самара Євгенія Вікторівна

Науковий керівник: д.психол.н., проф.

Лефтеров Василь Олександрович

Рецензент: д.юридич.н., проф.

Цільмак Олена Миколаївна

Одеса – 2024

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У КОНТЕКСТІ ПУБЛІЧНОГО УПРАВЛІННЯ ТА ЇХ ВПЛИВ НА СОЦІАЛЬНИЙ ТА ЕКОНОМІЧНИЙ РОЗВИТОК СУСПІЛЬСТВА.....	7
1.1. Потенціал сучасних інформаційних технологій у впровадженні інноваційних рішень у публічній сфері.	7
1.2. Новітні тенденції та технологічні інновації в галузі публічного управління.	19
Висновки за розділом 1.....	29
РОЗДІЛ 2. ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ	31
2.1. Системи електронного урядування: формування, організація та функціональні можливості.....	31
2.2. Роль інформаційних систем управління в оптимізації процесів публічного адміністрування.....	45
Висновки за розділом 2.....	55
РОЗДІЛ 3. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ІНТЕНСИВНОГО ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ	57
3.1. Загрози та ризики інформаційної безпеки в публічному секторі.	57
3.2. Стратегії забезпечення інформаційної безпеки в умовах використання сучасних інформаційних технологій в публічному управлінні.	66
Висновки за розділом 3.....	79
ВИСНОВКИ.....	81
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	87

ВСТУП

Актуальність дослідження.

Сучасний світ переживає революцію інформаційних технологій, яка неодмінно впливає на сфери громадського життя, включаючи публічне управління. Зростаюча комп'ютеризація та автоматизація процесів, пов'язаних з державним управлінням, обумовлює необхідність глибокого розуміння впливу інформаційних технологій на ефективність та безпеку адміністративних процедур.

Інформаційні технології в сфері публічного адміністрування стають не лише зручним інструментом для оптимізації процесів, але й важливим фактором для забезпечення інформаційної безпеки та конфіденційності важливих державних даних. Зростання кількості цифрових даних та їх обробка у великому масштабі роблять актуальними питання захисту та надійності інформаційних систем у сфері публічного адміністрування.

Особливу увагу привертає проблема забезпечення інформаційної безпеки у публічному секторі. Оскільки державні органи мають доступ до найбільш чутливої та конфіденційної інформації, їхні інформаційні системи стають об'єктом постійного уваги з боку хакерів та зловмисників. Ріст кількості кібератак та витоків даних свідчить про необхідність подальшого дослідження та вдосконалення заходів інформаційної безпеки в публічному управлінні.

Дослідження впливу інформаційних технологій на галузь публічного адміністрування є особливо важливим в контексті підвищення ефективності та прозорості державного управління. Правильно впроваджені технології можуть покращити якість надання послуг громадянам, спростити процедури та зменшити бюрократичний тиск.

Таким чином, дане дослідження є важливим в контексті сучасних викликів та потреб суспільства у підвищенні ефективності публічного адміністрування та

забезпеченні безпеки інформаційного простору.

Мета дослідження - полягає в комплексному аналізі взаємозв'язку сучасних інформаційних технологій, публічного управління та інформаційної безпеки з метою визначення оптимальних стратегій впровадження та використання цих технологій для забезпечення стійкого та ефективного функціонування публічного сектору.

Завдання дослідження.

Для досягнення поставленої мети, необхідно вирішити наступні завдання:

- Проаналізувати потенціал сучасних інформаційних технологій у впровадженні інноваційних рішень у публічній сфері.
- Вивчити новітні тенденції та технологічні інновації в галузі публічного управління.
- Дослідити системи електронного урядування та їхні основні принципи.
- Визначити роль інформаційних систем управління в оптимізації процесів публічного адміністрування.
- Проаналізувати загрози та ризики інформаційної безпеки в публічному секторі.
- Вивчити вплив інформаційних технологій на конфіденційність особистих даних у публічному секторі.
- Розглянути стратегії забезпечення інформаційної безпеки в умовах використання сучасних ІТ.

Об'єкт та предмет дослідження.

Об'єктом дослідження є процеси впровадження та використання інформаційних технологій в сфері публічного адміністрування. Предметом дослідження є інформаційні технології в галузі публічного адміністрування та їх вплив на інформаційну безпеку.

Методологічна основа дослідження ґрунтується на використанні

комплексного підходу до аналізу впливу інформаційних технологій на публічне управління. Застосування методів аналізу, синтезу та порівняльного аналізу дозволяє ретельно вивчити вплив інформаційних технологій у контексті публічного адміністрування. Крім того, використання експертних оцінок та моделювання дає можливість прогнозувати можливі наслідки впровадження новітніх технологій в систему публічного управління.

Дослідження базується на аналізі науково-методичної літератури, що дозволяє врахувати сучасні тенденції у розвитку інформаційних технологій та їх вплив на публічне управління. Також важливим елементом методологічної основи є аналіз практичних прикладів впровадження інформаційних технологій у сферу публічного адміністрування.

Наукова новизна дослідження.

Це дослідження відзначається науковою новизною завдяки комплексному підходу до аналізу впливу інформаційних технологій на публічне управління та їх взаємодію з інформаційною безпекою. Новаторство полягає у виявленні ключових факторів та принципів, які визначають ефективність використання інформаційних технологій в сфері публічного адміністрування. Крім того, дослідження надає новітні рекомендації щодо забезпечення інформаційної безпеки в контексті використання сучасних ІТ-рішень.

Надані результати та висновки можуть стати основою для подальших наукових досліджень у галузі публічного управління та інформаційних технологій, а також служити як практичний допоміжний матеріал для організацій та установ, що займаються впровадженням сучасних технологій у публічну сферу.

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 (77 найменування).

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У КОНТЕКСТІ ПУБЛІЧНОГО УПРАВЛІННЯ ТА ЇХ ВПЛИВ НА СОЦІАЛЬНИЙ ТА ЕКОНОМІЧНИЙ РОЗВИТОК СУСПІЛЬСТВА

1.1. Потенціал сучасних інформаційних технологій у впровадженні інноваційних рішень у публічній сфері.

В сучасному світі, публічне управління відіграє ключову роль у забезпеченні функціонування держави та задоволенні потреб суспільства. Це комплексна система, що включає в себе організаційну, правову, фінансову та інші компоненти. Основні аспекти публічного управління визначають його ефективність та вплив на життя громадян.

Першим важливим аспектом є прийняття рішень та планування. Управлінські органи розробляють стратегії та тактики впровадження політик, спрямованих на вирішення соціальних, економічних та інфраструктурних завдань. Цей процес вимагає компетентності, аналітичних здібностей та урахування інтересів різних груп населення.

Другим аспектом є моніторинг та оцінка реалізації управлінських рішень. Спеціальні служби відстежують динаміку реформ, аналізують результати та вносять необхідні корективи. Цей процес дозволяє уникнути негативних наслідків та максимізувати позитивний вплив управлінських рішень.

Однією з важливих складових є також забезпечення відкритості та доступності інформації. Прозорість у роботі органів влади є основою демократичного суспільства. Громадяни повинні мати можливість отримати достовірну та повну інформацію про діяльність органів влади.

До інших аспектів публічного управління можна віднести оптимізацію бюджетних видатків, реалізацію соціальних програм та підтримку ініціатив громадських організацій [1].

Однак, передусім, слід розглянути питання, чи є публічне управління тотожним із поняттям публічна сфера. Так, ці поняття мають тісний зв'язок, і одне не може існувати без іншого. Однак термін "публічна сфера" можна більш точно порівняти з визначенням "приватної сфери". У той час, коли приватна або домашня сфера – це сфера сімейного життя, друзів і особистих справ, публічна сфера – це місце, де відбувається вираження та обговорення ідей щодо спільних проблем і колективних соціальних інтересів. Термін "публічна сфера" часто вживається в однині, але "у великомасштабних диференційованих суспільствах пізнього модерну, не в останню чергу в контексті національних держав, пронизаних глобалізацією, ми повинні розуміти публічну сферу як складову багатьох різних просторів" [1]. Ось чому ми вважаємо за краще використовувати тут форму множини — публічні сфери — щоб визнати, що існує незліченна кількість форм фрагментації та конкуренції, як в публічних сферах поза, так і онлайн. І в глобальному контексті існує набір публічних сфер, які можуть варіюватися від глибоко демократичних до авторитарних [1].

Наведене вище міркування вже вказує на актуальність глобальної перспективи публічних сфер і технічної допомоги. Ми досліджуємо це, спочатку розглядаючи зв'язок у національному контексті, оскільки як до технічної допомоги, так і до академічного мислення про публічні сфери в основному підходять з точки зору національного прийняття політичних рішень та здійснення державного та публічного управління.

У цьому контексті Інформаційні технології (ІТ) оптимізували та полегшили спосіб, яким уряди ведуть свою діяльність та надають послуги громадянам. Вони відкрили нові можливості для покращення ефективності, транспарентності та відкритості в управлінні державними справами. Ми маємо достовірне розуміння того, що інформаційні технології є продуктом та корінням такого загального поняття, як інновації [2].

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

подальший розвиток та успішність. Поняття інновацій охоплює впровадження новаторських ідей, технологій, продуктів та методів у різних сферах життя. Це процес, який забезпечує конкурентоспроможність та стійкість суспільства у глобальному світі.

Однією з важливих галузей, де інновації грають визначальну роль, є економіка. Впровадження нових технологій та методів виробництва дозволяє підвищити продуктивність праці та покращити якість продукції. Це сприяє зростанню економіки та забезпечує підвищення рівня життя населення.

У сфері освіти та науки інновації також відіграють важливу роль. Впровадження нових методів навчання та досліджень сприяє підвищенню якості освіти та підготовки висококваліфікованих кадрів. Розвиток сучасних галузей науки та технологій стає ключовим фактором для подальшого прогресу суспільства [2].

Ще однією важливою сферою є медична галузь. Завдяки інноваційним методам діагностики та лікування з'являються нові можливості для рятування життів пацієнтів. Розробка нових лікарських препаратів та методів лікування вирішує проблеми, які ще недавно були невирішеними.

Окрім економіки та медицини, інновації мають значущий вплив на інші сфери життя. Наприклад, вони можуть змінити спосіб, яким ми взаємодіємо з інформацією, освітою, культурою та іншими аспектами суспільства [2].

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].

Розвиток інформаційних технологій як міцний стержень інновацій надає безліч можливостей для трансформації суспільства та управління ним. Процеси

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

- Смарт-міста та інфраструктура: З використанням сенсорів, технологій Інтернету речей (IoT) та збірних даних, міста можуть оптимізувати управління енергоспоживанням, транспортом, водопостачанням тощо. Наприклад, системи "розумних світлофорів" можуть підлаштовувати світлофори в залежності від щільності руху [9].

- Електронне здоров'я: Впровадження електронних медичних карт та телемедицини дозволяє покращити доступ до медичних послуг та моніторингу стану пацієнтів [8].

- Електронне освітнє середовище: Розробка платформ для дистанційного навчання, адаптованих до потреб різних груп населення, сприяє розвитку освіти.

- Фінансові технології (FinTech): Інноваційні платіжні системи та електронні гроші забезпечують швидке та зручне проведення фінансових операцій.

- Соціальні мережі та спільноти: Сучасні комунікаційні платформи забезпечують надійний канал для обміну інформацією між владою та громадянами.

- Електронна демократія: Засоби електронного голосування та публічні консультації надають можливість громадянам брати участь у процесах управління.

Ці інновації можуть сприяти покращенню ефективності державних служб, підвищенню рівня сервісу для громадян і бізнесу, а також покращенню якості прийняття управлінських рішень. Проте, разом з ними виникають і питання щодо приватності, кібербезпеки та етичних аспектів використання особистих даних [5].

Використання інформаційних технологій (ІТ) у сфері публічного управління відкриває перед суспільством безліч переваг та, одночасно, вносить

свої обмеження. Переваги включають:

- Підвищення ефективності та швидкості роботи: Використання ІТ дозволяє автоматизувати багато процесів, що раніше вимагали значних зусиль та часу. Наприклад, електронні системи обліку та аналізу даних дозволяють швидко здійснювати моніторинг різних показників.
- Підвищення доступності послуг: Електронні платформи дозволяють громадянам отримувати необхідну інформацію та послуги онлайн, що робить їх більш доступними для різних соціальних груп та регіонів.
- Можливість здійснення аналізу та прогнозування: Аналітичні інструменти на базі ІТ дозволяють урядовим структурам проводити більш детальний аналіз різних аспектів суспільного розвитку, що сприяє кращому прийняттю управлінських рішень.
- Посилення прозорості та відкритості: Електронні платформи для оприлюднення інформації про рішення та дії уряду дозволяють громадянам бути більш обізнаними та активними у впливі на політику.
- Зменшення витрат: Оптимізація процесів та впровадження електронного документообігу може призвести до зменшення бюрократичних витрат [6].

Проте, важливо врахувати обмеження використання ІТ:

- Кібербезпека та конфіденційність даних: Розробка механізмів захисту особистих даних та запобігання кібератакам стає важливим завданням.
- Доступність та ексклюзивність: Важливо не залишити позаду тих, хто не має доступу до ІТ або не володіє необхідними навичками для користування ними [7].
- Залежність від технологій: При недостатній резервованості або неправильному впровадженні, може виникнути небезпека втрати даних або збоїв у роботі систем.
- Етичні аспекти: Використання ІТ вимагає вирішення питань етики та

правового регулювання, особливо в контексті збору та обробки особистих даних.

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

Дослідження використання інформаційно-комунікаційних технологій (ІКТ) у публічному управлінні вказують на те, що впровадження електронного урядування є одним із ключових інструментів досягнення ефективної діяльності публічного управління. Використання сучасних ІКТ дозволяє здійснювати якісні зміни в діяльності органів публічного управління, зокрема, впроваджувати принципово нові форми діяльності цих структур.

Одна з головних переваг ІКТ полягає у можливостях для розширення доступу до послуг та зменшення бюрократичних процедур. Наприклад, електронне голосування може значно спростити процес проведення виборчих кампаній, особливо в умовах складного військово-політичного становища в Україні. Громадськість може бути більш активною та залученою до прийняття рішень через використання онлайн-консультацій і голосувань [7].

ІКТ також можуть бути корисними для публічного управління за наступних обставин:

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

Однак впровадження систем електронного урядування стикається з рядом проблем, таких як обмежене поширення мережі Інтернет, недостатнє фінансування процесу інформатизації, консерватизм і бюрократизм чиновників тощо. Особливостями використання сучасних ІКТ у публічному управлінні є змішаний документообіг та повільний перехід до повного електронного документообігу. Використання соціальних мереж є перспективним комунікативним каналом між владою та суспільством, який відкриває багато

нових можливостей для органів публічного управління.

Згадане дослідження також вказує на те, що сучасний стан розбудови інформаційного суспільства та сфери ІКТ в Україні, порівняно зі світовими тенденціями, є недостатнім і не відповідає стратегічним цілям розвитку України. Сьогодні в системі публічного управління України є нагальна потреба у використанні нових інструментів, методів і технологій, спрямованих на підвищення її ефективності [10].

Повертаючись до теми соціальних, демографічних і політичних викликів, у якості прикладу можна розглянути інформаційно-технологічні рішення щодо боротьби із світовою пандемією COVID-19. Вказаний кейс включає як реалізовані інновації, так і пропозиції, які не були впроваджені, однак мають обґрунтоване право на існування.

Пандемія COVID-19 спричинила величезний вплив на системи охорони здоров'я, підприємства, школи та економіку. Телемедицина, дистанційна робота та онлайн-освіта стали важливими елементами для допомоги суспільству уповільнити поширення коронавірусу [11]. Пандемія стала тригером що породив стрімкий попит використання інноваційних технологій для подолання шкоди, завданої COVID-19 нашому життю [11]. Це не лише відкрило можливості для просування технологічних рішень, але й надало рідкісну можливість вивчати дослідження та практику технологій, включаючи управління інформацією, методи роботи, а також розробку та використання технологій [12]. Швидкий перехід на телемедицину, дистанційну роботу та онлайн-освіту у відповідь на загрозу коронавірусу є нагадуванням про те, що цифрові технології приносять багато переваг і можуть відігравати важливу роль в управлінні та зменшенні ризиків, спричинених локдауном під час пандемії та навіть після неї. Добре відомо, що інформаційні системи та інформаційні технології (ІС/ІТ) відіграють важливу роль в охороні здоров'я, підтримці прийняття клінічних рішень, реагуванні на надзвичайні/кризові ситуації та управлінні ризиками [13]. "Багато

фахівців у сфері інформаційних технологій вживали різні заходи для допомоги у боротьбі з пандемією, включаючи розробку продуктів для боротьби з вірусом, відстеження та прогнозування його поширення, а також захист лікарень від кібератак. Дослідники інформаційних систем і технологій внесли свій внесок у глобальні зусилля з боротьби з COVID-19 та іншими епідеміями, використовуючи свій попередній досвід у сфері реагування на кризи, прийняття рішень, віддаленої роботи, управління віртуальними командами, аналізу великих масивів даних тощо. Зараз ще не вистачає даних дослідження в області інформаційних систем, які допомагають в боротьбі з COVID-19 або іншими світовими кризами у медичному секторі. Незважаючи на послаблення загрози коронавірусу, передові науковці, інженери, медичні працівники, спеціалісти інформаційних технологій продовжують працювати в цьому напрямку, сподіваючись досягти ще більш вагомих результатів [13].

Світова практика розвитку освіти в контексті потенціалу сучасних інформаційних технологій підкреслює важливість впровадження інновацій у публічній сфері. Аналітична доповідь ЮНЕСКО "Програма сталого розвитку після 2015 року" визначає, що у новій інформаційній ері вища освіта повинна стати ключовим елементом прогресу, а інновації у різних сферах суспільної діяльності повинні включати в себе високий динамізм швидкої зміни та адаптації знань, зокрема у сфері інформаційних технологій [14]. В такому контексті зростає суспільна значущість держави у забезпеченні доступу до якісної освіти, високого рівня знань, можливості набуття відповідних навичок та компетенцій через забезпечення академічної мобільності та свободи вищих навчальних закладів [14].

В умовах формування інноваційного суспільства функціональні особливості освіти включають не лише передачу студентам обсягу знань і вмінь, накопичених за попередні роки, але й розвиток їхньої здатності сприймати та використовувати на практиці нові наукові ідеї, засоби та методи.

Сучасний світ, де живе людина, стає складним і суперечливим. Для формування розумної стратегії власного життя необхідний достатньо високий інтелектуальний і творчий потенціал, високий професіоналізм. Отже, одним із ключових завдань вищої школи є особистісно-професійний розвиток студентів. Розвиток повинен бути прогресивним, а процес набуття знань повинен включати застосування інноваційних рішень.

На сьогоднішній день термін "Soft skills" зарубіжного походження набуває популярності. Це відноситься до особистих якостей та навичок. На відміну від технічних чи професійних вмінь, це не просто знання, якими ви володієте, а поведінка, яку ви демонструєте у різних ситуаціях. "Soft skills" включають будь-яку навичку, яку можна віднести до особистісних рис або звичок [15]. Навички міжособистісного спілкування та комунікативні навички є більш конкретними категоріями софт-скіллів, які багато роботодавців шукають у кандидатах на роботу [15]. Ось кілька з найбільш затребуваних софт-скіллів:

- Ефективні комунікаційні навички.
- Командна праця.
- Надійність.
- Адаптованість.
- Управління конфліктами.
- Гнучкість.
- Лідерство.
- Вирішення проблем.
- Відкритість новому.
- Творчий підхід.
- Трудова етика.
- Чесність [15].

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). Освіта та наука, які виступають чинниками розвитку публічної сфери, в умовах впровадження інноваційних процесів, мають враховувати цінність "Soft skills" та включати відповідні соціологічні та психологічні тренажери, спрямовані на розвиток визначених навичок у різних категорій населення [15].

Якщо мова заходить про педагогічну практику, слід відзначити, що вона вимагає створення відносно простого, а водночас максимально універсального інструментарію для здійснення особистісно-професійного розвитку студентів. Цей інструмент повинен розкривати структуру та динаміку цього розвитку в інноваційних технологіях навчання і моделювання освітнього середовища. У цьому контексті необхідно переглянути основні компоненти освіти: зміст, форми, методи, технології навчання, методичне забезпечення (зокрема підручники) та функції вчителя [16].

Поняття "педагогічні технології" трансформувалося в нові поняття: освітні технології, педагогічні технології, технології навчання. Освітні технології відображають загальну стратегію розвитку освіти, єдиний освітній простір, призначені для прогнозування розвитку освіти, конкретного проектування та планування, прогнозування результатів, а також визначення відповідних освітніх цілей стандартів. Прикладами освітніх технологій є концепції освіти та системи освіти [16].

Якщо освітні технології відображають стратегію освіти, то педагогічні втілюють тактику її впровадження в освітній процес шляхом впровадження моделей останнього та ідентичних моделей управління цим процесом. Наприклад, модель особистісно-орієнтованого розвивального навчання, модульно-розвивального навчання, проблемного навчання тощо. Отже, педагогічна технологія відображає модель освітнього та управлінського процесів навчального закладу та поєднує зміст, форми та засоби кожного з них [16].

Межі застосування інновацій у публічній сфері та розвитку держави і

суспільства здаються відсутніми. Ми розглянули лише декілька впроваджених процесів, які не містять навіть маленького відсотку стратегічного потенціалу інноваційної новизни. Неможливо недооцінити користь Інтернету як простору публічності.

Обговорення демократичного потенціалу Інтернету не може задовольнитися простим переліком його позитивних або внутрішніх рис, таких як швидкість, масштаб чи "анархічна" природа. Це стосується і його негативних ефектів чи наслідків, таких як дезагредований характер чи анонімність. Взяті разом, обидва ці міркування заперечують розглядати Інтернет як варіацію існуючої преси та національної публічної сфери. Його комп'ютерно-опосередкована комунікація відкриває новий вид "розподільчої", а не єдиної публічної сфери з новими формами взаємодії.

Під "розподільчим" розуміється, що комп'ютерне посередництво у формі Інтернету "децентралізує" публічну сферу; це громадськість громадськості, а не чітко уніфікована та охоплююча публічна сфера, в якій беруть участь усі комунікатори. Замість того, щоб просто входити в існуючу публічну сферу, Інтернет стає публічною сферою лише через агентів, які беруть участь у рефлексивній і демократичній діяльності [17].

Щоб Інтернет міг створити нову форму публічності, що виходить за межі простої сукупності всіх своїх користувачів, він повинен бути розроблений як публічна сфера тими, хто демонструє риси діалогу та виявляє зацікавленість у його публічності.

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 [17].

Є кілька причин вважати, що існуючі демократичні інститути недостатньо

справляються з цим завданням. Держави сприяють приватизації різноманітних медіа-просторів для комунікації, включаючи не лише Інтернет, а й частоти мовлення. Навіть якщо Інтернет, за своєю суттю, не є анархістичним, і навіть якщо держави були б готові робити більше для захисту публічного характеру кіберпростору, залишається відкритим питання, чи може ця форма комунікації функціонувати за межами того, як державний суверенітет організовує простір і час, включаючи публічний простір і час обговорення [18].

Таким чином, сучасні інформаційні технології відкривають безмежні можливості для впровадження інноваційних рішень у сфері публічного управління. Зокрема, їхній потенціал надзвичайно важливий для ефективності та транспарентності діяльності державних та адміністративних структур. Специфічні переваги використання інформаційних технологій включають можливість оптимізувати прийняття рішень, аналізуючи великі обсяги даних. Це дозволяє ухвалювати кращі та обґрунтовані рішення, що відповідають реальним потребам суспільства. Крім того, впровадження електронних платформ і сервісів значно спрощує взаємодію громадян з державними органами. Це робить послуги більш доступними та зручними для населення. Розвиток сучасних інформаційних технологій також сприяє інноваціям у сфері публічного управління. Вимагається постійне вдосконалення та розвиток технологій, що стимулює створення новаторських рішень та продуктів для оптимізації державного управління. З використанням ІТ можливо створити відкриті платформи для публікації інформації про діяльність урядових структур, що сприяє прозорості та відкритому доступу до важливих даних для громадськості.

Інформаційні технології надають можливість раціонально розподіляти та використовувати ресурси, що є особливо важливим у ситуаціях фінансової обмеженості. Загалом, сучасні інформаційні технології є потужним інструментом для оптимізації публічного управління та досягнення кращих результатів у наданні послуг громадянам. Впровадження цих технологій потребує системного

підходу та постійного оновлення, але при цьому надає найважливіші переваги для суспільства в цілому."

1.2. Новітні тенденції та технологічні інновації в галузі публічного управління.

Публічне управління є неодмінною складовою сучасного суспільства. Його роль та значення визначаються наявністю системи ефективних інструментів, спрямованих на вирішення соціально-економічних завдань та забезпечення гармонійного розвитку країни. У цьому розділі розглядаються основні поняття та принципи, що лежать в основі публічного управління, його складові елементи та мета.

Для початку, важливо розглянути основне визначення публічного управління. За сучасними уявленнями, публічне управління - це система організаційних та функціональних заходів, спрямованих на реалізацію стратегічних цілей та завдань суспільства. Воно включає в себе усі аспекти державного впливу на соціально-економічні та політичні процеси [19].

Для забезпечення ефективного функціонування публічного управління необхідно дотримуватися низки важливих принципів. Один із найважливіших - це принцип законності та легітимності. Він передбачає, що управлінські органи повинні діяти відповідно до чинного законодавства та мати відповідний суспільний легітимний мандат.

Наступним ключовим принципом є прозорливість та відкритість. Вони передбачають доступність інформації про рішення та дії влади для громадськості. Цей принцип є гарантом демократичного характеру управління та можливості громадян впливати на прийняття важливих рішень.

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 [20, с. 125].

В системі публічного управління виділяють декілька ключових складових. Перша складова - це органи виконавчої влади, які несуть відповідальність за реалізацію прийнятих рішень та програм. До їхніх обов'язків входить контроль за дотриманням законів та стандартів.

Друга складова - це органи законодавчої влади, які визначають загальні принципи функціонування системи та приймають закони. Вони виступають основним органом представництва громадян у владних структурах.

Третьою важливою складовою є участь громадських організацій та ініціативних груп, які можуть впливати на прийняття рішень через активну участь у громадському діалозі.

Головною метою публічного управління є забезпечення стабільності та розвитку суспільства. Це включає в себе не лише гарантування прав та свобод громадян, але й створення сприятливих умов для економічного зростання та забезпечення соціальної справедливості.

Під час реформування в Україні на початку 1990-х років уявлення про "державне управління" стало цілеспрямованим та організованим впливом держави на суспільні процеси. Це враховує не лише діяльність органів влади та посадових осіб, але і вплив організаційних структур, що спеціалізуються на різних сферах матеріальних, соціальних та культурних цінностей та продуктів.

Хоча українське законодавство іноді використовує термін "державне управління" замість "публічного управління", останнє є більш сучасним та відображає модель управління суспільством, враховуючи його відмінності від традиційного "державного управління" [21, 27].

Незважаючи на багатогранність та різноманіття сучасного суспільства, публічне управління залишається невід'ємною частиною кожної країни, що дбає про реалізацію інтересів та потреб громадян. 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.

Однією з ключових тенденцій розвитку публічного управління є посилення його інформаційної складової. Сучасні технології та зростання доступності інформації надають можливість ефективно впливати на прийняття управлінських рішень, враховуючи потреби різних соціальних груп та особистостей. Публічні службовці мають можливість оперативно аналізувати дані та реагувати на зміни в суспільстві [22].

Ще однією важливою тенденцією є підвищення відкритості та прозорості управлінських процесів. Громадськість має право бути поінформованою про діяльність органів влади та мати можливість впливати на ухвалення стратегічних рішень. Співпраця громадян та органів влади на різних етапах управлінського процесу є важливим аспектом сучасного публічного управління [22].

Крім того, слід відзначити зростання ролі місцевого самоврядування у системі публічного управління. Відповідно до Конституції України, місцеві органи самоврядування є носіями місцевого самоврядування та забезпечують вирішення питань місцевого значення. Їх роль в наданні якісних послуг та задоволенні потреб громадян стає надзвичайно важливою. Зростає значущість стратегічного планування у публічному управлінні. Розробка та впровадження стратегічних документів дозволяє краще координувати дії різних гілок влади та спрямовувати їх на досягнення загальних цілей суспільства.

Враховуючи вищезазначені тенденції, слід підкреслити, що сучасне публічне управління є динамічним та постійно змінюється під впливом різних факторів. Його розвиток вимагає від службовців високого рівня компетентності, а від органів влади – готовності до інновацій та впровадження сучасних підходів у управлінській діяльності [23].

Сучасне динамічне бізнес-середовище також вимагає від організацій

постійно адаптуватися та впроваджувати нові підходи для забезпечення конкурентоспроможності. У цьому контексті інноваційне управління стає ключовим чинником, що дозволяє структурувати та ефективно впроваджувати новаторські ідеї, технології та методи в усі сфери організаційної діяльності. Поняття інновації ми вже розглянули у попередньому підрозділі, а що таке інноваційне управління?

Інноваційне управління - це комплексна система керування, спрямована на створення умов для стимулювання розвитку та ефективного впровадження інновацій у всі сфери діяльності організації. Для більш глибокого розуміння стратегічного управління доцільно розглянути його основні принципи [28].

1. Стратегічне бачення. Першим ключовим принципом інноваційного управління є розробка чіткої та амбіційної стратегії. Ця стратегія повинна визначити мету та напрямок інноваційних зусиль, враховуючи як внутрішні, так і зовнішні фактори. Важливо встановити конкретні цілі, завдання та очікувані результати, а також визначити шляхи досягнення цих цілей. Як компас, стратегія служить орієнтиром для всієї організації в процесі інноваційного розвитку.

2. Лідерство та підтримка керівництва. Цей принцип покладає відповідальність на керівництво організації у активному стимулюванні та підтримці інноваційних ініціатив. Лідери повинні бути відкритими до нововведень, виявляти ініціативу у їх впровадженні та бути прикладом для інших співробітників. Їхня активна участь та зацікавленість в інноваціях створює потужний мотиваційний сигнал для всього колективу [28].

3. Залучення персоналу. Інноваційне управління передбачає активну участь всіх працівників організації у створенні та впровадженні нововведень. Важливо створити механізми для збору та аналізу ідей від персоналу, надати можливість працівникам брати участь у інноваційних проєктах та нагороджувати їх за внесок у цей процес.

4. Системний підхід. Інноваційне управління повинно бути вбудоване

в загальну систему керування організацією. Це передбачає інтеграцію інновацій у всі аспекти діяльності компанії – виробництво, маркетинг, фінанси, кадри тощо. Важливо враховувати вплив інновацій на внутрішні та зовнішні аспекти бізнес-процесів, а також спрямувати всі зусилля на досягнення спільної мети.

5. Інноваційна культура. Створення сприятливого середовища для інновацій – ключовий аспект ефективного управління. Це передбачає створення атмосфери відкритості, підтримки та визнання для творчих ідей. Важливо надихати працівників на пошук новаторських рішень та створення умов для їхнього розвитку [28].

6. Партнерство. Успішне інноваційне управління включає в себе встановлення партнерських відносин з іншими компаніями, дослідницькими установами та стартапами. Це дозволяє обмінюватися знаннями та технологіями, сприяючи більш ефективному впровадженню інновацій.

7. Оцінка та моніторинг. Контроль та оцінка результатів інноваційних проектів є важливою складовою успіху. Систематичний аналіз ефективності дозволяє виявляти проблеми та вносити необхідні корективи. Важливо враховувати як кількісні, так і якісні показники успішності, а також адаптувати стратегію відповідно до отриманих результатів [28].

Ці принципи є основою для ефективного інноваційного управління в організації. Важливо розуміти, що інновації – це постійний процес, який вимагає стійкого вдосконалення та адаптації. Тільки такий підхід дозволяє утримувати конкурентні переваги та забезпечувати стабільний розвиток організації в умовах постійних змін на ринку [29].

Інноваційне управління також пов'язане з певним ризиком та невизначеністю. Важливо бути готовими до експериментів та вміти вчитися на власних помилках. Правильне вирішення цих викликів дозволяє створити гнучку та адаптивну організацію, здатну ефективно конкурувати та розвиватися в сучасних умовах [30].

Публічне управління є ключовим чинником суспільного розвитку у всіх країнах. У сучасних умовах відбувається стрімкий розвиток технологій, що суттєво впливає на підходи та методи управління суспільними процесами. Технологічні інновації в публічному управлінні стають все більш важливими для забезпечення ефективного та результативного функціонування сучасних адміністративних систем.

Технологічні інновації у сфері публічного управління охоплюють впровадження сучасних інформаційних технологій, аналіз даних в реальному часі, використання штучного інтелекту, а також розвиток електронних платформ для надання громадських послуг. Принципи технологічних інновацій у публічному управлінні:

1. Цифрова трансформація – один із ключових принципів. Вона передбачає перехід від традиційних адміністративних процедур до використання сучасних інформаційних технологій для оптимізації роботи державних установ [31].

2. Відкриті дані. Забезпечення доступу до відкритих даних є ще одним важливим принципом. Це сприяє підвищенню прозорості та відкритості у діяльності публічних установ перед громадськістю [31].

3. Електронне урядування. Впровадження електронного урядування дозволяє здійснювати адміністративні послуги онлайн, полегшуючи взаємодію між державою та громадянами [29].

4. Інноваційний лідер. Важливо мати особу, відповідальну за впровадження технологічних інновацій в адміністративний процес. Інноваційний лідер сприяє координації та впровадженню нововведень [30].

Інновації в публічному управлінні можуть стати важливим інструментом для досягнення ефективності та результативності в управлінні державними справами. Україна не є винятком, і існує багато прикладів успішної реалізації інновацій в публічному управлінні в Україні. Наприклад, відкритий бюджет

України є одним із найбільш успішних прикладів використання інновацій в публічному управлінні в Україні. Іншим прикладом є впровадження електронного урядування в Україні, що дозволило зменшити корупцію та підвищити ефективність управління державними справами. Крім того, в Україні були впроваджені інноваційні методи управління місцевими фінансами, такі як електронні системи оподаткування та бюджетування, що дозволило підвищити ефективність управління місцевими фінансами [29, 32].

Розглянемо більш детально перший державний проект, якому ми приділимо увагу - програмний продукт "Прозоро". "Прозоро" - це електронна система публічних закупівель в Україні, створена з метою забезпечення прозорості та ефективності у сфері державних закупівель. Система "Прозоро" дозволяє державним та комунальним замовникам оголошувати тендери на закупівлю товарів, робіт та послуг, а представники бізнесу змагаються на торгах за можливість поставити це державі. Все, що відбувається на торгах, може побачити будь-хто на спеціалізованому веб-порталі. Ця система є одним із найбільш успішних прикладів використання інновацій в публічному управлінні в Україні [33].

Прикладом зарубіжного досвіду у сфері інновацій у державній сфері є "Smart Dubai" - це програма, яка була запущена в 2014 році з метою зробити Дубай більш "розумним" містом. Програма базується на використанні новітніх технологій, таких як блокчейн, штучний інтелект та аналіз даних, для поліпшення якості життя мешканців та відвідувачів міста. "Smart Dubai" включає різні ініціативи, такі як "DubaiNow", "DubaiPay" та "DubaiID", які дозволяють громадянам та підприємцям отримувати доступ до різних державних послуг онлайн. Програма також включає ініціативи з покращення транспортної системи, енергоефективності та екології [34].

Програмний продукт "Smart Dubai" є частиною стратегії "Dubai Plan 2021", яка була запущена з метою зробити Дубай одним з "найщасливіших" та найбільш

інноваційних міст світу. "Smart Dubai" допомагає зробити Дубай більш доступним та зручним для мешканців та відвідувачів міста, а також зменшує кількість паперової роботи та сприяє економії часу та коштів [35].

У розрізі світової практики неможливо не згадати Естонію та її електронне урядування. Система Estonian e-Government є однією з найбільш успішних у світі. Запроваджена в 2001 році, вона стала прикладом для наслідування для багатьох країн [36]. Основні компоненти системи Estonian e-Government включають:

- X-Road: Це розподілена інформаційна платформа, яка дозволяє різним системам спілкуватися між собою. Наприклад, поліція може отримати доступ до даних з системи охорони здоров'я, податкової служби або реєстру бізнесу, а також навпаки. X-Road дозволив збільшити глибину співпраці між державними організаціями та зменшити кількість паперової роботи, щоб працівники державних органів могли сконцентруватися на завданнях, які потребують людської уваги [36].

- Електронні державні послуги: Більшість державних послуг в Естонії доступні онлайн. Це дозволяє громадянам та підприємцям отримувати доступ до послуг швидко та зручно, таких як реєстрація місця проживання, подання заяв на отримання паспорта або водійського посвідчення, а також реєстрація компаній онлайн.

- Електронні ідентифікатори: Естонія має найбільш розвинуту національну систему ID-карток у світі. Ці карти не тільки надають громадянам доступ до всіх безпечних електронних послуг в країні, але й дозволяють підписувати документи та голосувати виборцям онлайн [36].

Ці елементи дозволяють громадянам та підприємцям отримувати доступ до державних послуг швидко та зручно, а також зменшують кількість паперової роботи, допомагаючи державним службовцям сконцентруватися на завданнях, які потребують людської уваги, а не на рутинних процедурах [36].

Повертаючись до вітчизняних проривів, звернемо увагу на один із

найуспішніших проектів у впровадженні інновацій у сфері інформаційних технологій у структурі публічного управління.

Платформа "Дія" (походження від «Держава і я», англ. Diia) — мобільний додаток та веб-сервіс, що є частиною ініціативи цифрового перетворення в Україні і був розроблений Міністерством цифрової трансформації України. Проект був представлений вперше у 2019 році та офіційно введений в експлуатацію у 2020 році [32, 37].

За допомогою додатка можна зберігати водійські посвідчення, внутрішні та міжнародні паспорти та інші документи у електронному вигляді, а також надсилати їхні копії при отриманні банківських чи поштових послуг, реєстрації в готелях та в інших ситуаціях. Крім того, за допомогою "Дія" (через додаток або веб-сервіс) можна отримати такі державні послуги, як "єМалятко" (інтегрована послуга при народженні дитини), реєстрація бізнесу та ФОП онлайн, оплата податків та подання декларацій, електронний підпис для будь-яких документів, зміна місця проживання та інше. Планується, що до 2024 року 100% державних послуг будуть доступні через "Дія" [32, 37].

Станом на листопад 2023 року платформою вже користуються понад 17 мільйонів людей. На веб-сервісі доступно більше 70 послуг, а в додатку - 9 послуг та 15 електронних документів. Крім того, на офіційному порталі "Дія" анонсовано більше 90 проектів [37].

На муніципальному рівні також хотілося б згадати програму безпеки дорожнього руху в м. Одесі. Це міська цільова програма, яка спрямована на зниження кількості дорожньо-транспортних пригод, підвищення якості дорожньої інфраструктури та підвищення рівня безпеки учасників 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. Запровадження мультимодальної цифрової транспортної моделі міста. Перехід на сучасні ІТ-інструменти планування та прогнозування транспортної інфраструктури міста. Моделювання та прогнозування для прийняття зважених, економічно обґрунтованих рішень.

4. Впровадження програмного забезпечення для мікромоделювання режимів роботи світлофорних об'єктів, дорожніх перехресть та інших елементів транспортної інфраструктури міста.

5. Початок облаштування безпечної інфраструктури міста.

6. Перехід на дорожню розмітку із пластику [38].

Однак у призмі нашого дослідження нас цікавить ефективне, з точки зору публічного управління, рішення з інтеграції міських систем у сервіс «Штрафи UA». Штрафи UA - це національний сервіс, який дозволяє перевіряти наявність штрафу (патрульні, з камер спостереження, за паркування в ряді міст країни) та швидко і зручно оплачувати його. Для зручності громадяни можуть використовувати сайт, додаток для Android, або Telegram-бота для перевірки штрафів за номером авто або посвідченням водія. За інформацією Одеської міської ради менш ніж за тиждень фіксується більше ніж 2 тисячі порушень правил паркування, що дозволяє поповнювати міський та державний бюджет майже 1 млн. грн [38].

У сучасному світі динамічні зміни та виклики в суспільстві вимагають постійного аналізу та адаптації системи публічного управління до нових умов. 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.

Другою важливою тенденцією є підвищення ролі громадськості у процесі

прийняття та реалізації рішень. Залучення громадських організацій та активних громадян до діалогу з владою сприяє більш ефективному вирішенню проблем та врахуванню реальних потреб суспільства.

Також важливо відзначити тенденцію до розширення міжнародного співробітництва у сфері публічного управління. Обмін досвідом та впровадження кращих практик з інших країн дозволяє уникнути повторних помилок та досягти більшого успіху в управлінні.

Зростання значення прозорості, відкритості та відповідальності стають основними принципами сучасного публічного управління. Громадськість очікує від влади відкритості в прийнятті рішень та відкритої звітності про їх реалізацію. Усі ці тенденції та інновації в сфері публічного управління спрямовані на покращення якості життя громадян, забезпечення стабільності та розвитку суспільства. Важливо надати пріоритет впровадженню сучасних технологій та підтримці громадськості в управлінні, щоб досягти цих цілей.

Висновки за розділом 1.

Розділ 1 присвячений ретельному аналізу сучасних інформаційних технологій та їхнього впливу на публічне управління з метою сприяння справедливому соціальному та економічному розвитку суспільства. Здійснений огляд ключових аспектів визначає важливі напрямки для подальшого розвитку та впровадження інновацій.

1. Аналіз показав, що інформаційні технології стають ключовим інструментом для впровадження інновацій в сфері публічного управління. Вони не лише оптимізують рутинні процеси, але й створюють умови для швидкого та ефективного вирішення соціально-економічних завдань. Потенціал технологій полягає в їхній здатності забезпечувати точність, прозорість та швидкість у прийнятті та виконанні управлінських рішень.

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.

РОЗДІЛ 2. ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ

2.1. Системи електронного урядування: формування, організація та функціональні можливості.

У світі, який стрімко розвивається в епоху цифрових технологій, системи електронного урядування (СЕУ) стають необхідним елементом сучасного адміністративного ландшафту. Ці системи визначають новий стандарт управління, де технології використовуються для оптимізації процесів, забезпечуючи ефективну взаємодію між владою та громадою. Однак, перед тим як ми вивчимо сутність і функціональні можливості СЕУ, важливо зануритися в історію їх становлення та вивчити основні аспекти їх структури та організації, розглядати етапи формування, принципи організації та широкий спектр функціональних можливостей, які пропонують сучасні системи електронного урядування. Також, ми розглянемо виклики, з якими стикаються ці системи, та розглянемо перспективи їхнього майбутнього розвитку в умовах постійної динаміки технологічного прогресу.

Система електронного урядування – поняття досить нове, однак вже має довгу історію становлення. Для чіткого розуміння ми виділили два основних етапи розвитку систем електронного урядування у світі.

Перший період становлення електронного урядування. Початок розвитку електронного урядування (e-government) можна відслідкувати ще в 1960-70-х роках, коли комп'ютери почали використовуватися для обробки даних в адміністративних процесах. Спроби автоматизації та впровадження електронних систем в різних країнах були обмеженими, проте цей період визначав стартові

кроки в напрямку електронної трансформації урядових служб.

Другий етап - це етап Інтернет-революції та формування Інтернет-уряду. У 1990-2000-х роках з поширенням Інтернету виникла нова ера для електронного урядування. Країни, такі як США, Велика Британія, Сінгапур та Швеція, активно розробляли та впроваджували електронні сервіси для спрощення взаємодії громадян з владою. Програми, такі як "e-Government Action Plan" в Європейському Союзі, підтримували впровадження інформаційних технологій в адміністративних структурах. План дій з електронного урядування - це ініціатива Європейського Союзу, спрямована на модернізацію цифрових державних служб, щоб зробити ЄС кращим місцем для роботи, проживання та інвестування. Метою плану є забезпечення того, щоб люди по всьому ЄС повністю користувалися перевагами цифрових державних служб [39].

У 21 столітті спостерігається зростання глобальної тенденції впровадження електронного урядування. Країни розробляють стратегії та державні програми для покращення доступності та ефективності електронних послуг. Наприклад, Естонія визначилася як лідер у впровадженні e-Government, забезпечуючи інтерактивність та зручність громадянських послуг через електронні платформи.

Щоб зрозуміти суть системи електронного урядування, розглянемо її основні моделі реалізації, а також їх переваги та недоліки.

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

1. Централізована модель: Деякі країни, такі як Сінгапур, вибирають централізовану модель, де урядові послуги надаються через єдиний центр керування. Це сприяє стандартизації та ефективному управлінському контролю, але може обмежувати локальні особливості [39].

Перевагами такої моделі є:

- ефективність управління: централізована модель спрощує управління електронним урядуванням, що дозволяє швидше впровадження та

стандартизацію послуг;

- оптимізація ресурсів: зменшення дублювання функцій та ресурсів, оскільки всі електронні сервіси надаються через єдиний центр [40].

Однак вона також має деякі недоліки:

- бюрократія: можливість збільшення бюрократії та важкопрохідних процедур через централізовану систему;
- обмеженість локальних потреб: може бути менш гнучкою у відповіді на конкретні потреби різних регіонів чи груп населення [40].

2. Децентралізована модель: інші країни, наприклад, Канада, вибирають більш децентралізований підхід, де різні рівні влади мають свої власні системи електронного урядування. Це може забезпечувати більшу гнучкість, але вимагає більшої координації [39].

Перевагами такої моделі є:

- гнучкість: децентралізована модель може бути більш адаптованою до місцевих особливостей та потреб різних груп громадян;
- 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.

Детальне вивчення цих переваг і недоліків є важливим для визначення оптимального підходу до реалізації електронного урядування в контексті конкретної країни чи регіону. Рішення повинні враховувати специфіку культур, соціально-економічних умов та потреб громади [42].

У сучасному світі ефективне функціонування Систем Електронного

Урядування (СЕУ) визначається його організаційною структурою, яка забезпечує розподіл влади та функцій між різними рівнями та галузями влади. Структура Систем Електронного Урядування (СЕУ) - це комплексна система, яка забезпечує взаємодію між державними органами та громадянами за допомогою інформаційних технологій. Система складається з наступних компонентів:

- Компоненти інфраструктури: Це компоненти, які забезпечують функціонування СЕУ. Вони включають в себе компоненти забезпечення безпеки, компоненти забезпечення доступності, компоненти забезпечення інтеграції та компоненти забезпечення масштабованості.

- Компоненти послуг: Це компоненти, які забезпечують надання послуг громадянам та бізнесу. Вони включають в себе компоненти надання послуг, компоненти забезпечення якості послуг та компоненти забезпечення доступності послуг.

- Компоненти інформаційної системи: Це компоненти, які забезпечують збір, обробку та зберігання інформації. Вони включають в себе компоненти збору інформації, компоненти обробки інформації та компоненти зберігання інформації [42].

Структура Системи Електронного Урядування (СЕУ) може відрізнятися в залежності від країни та її потреб [43].

Сучасні глобальні тенденції вказують на використання передових технологій у розвитку інноваційного електронного урядування. Штучний інтелект, блокчейн, аналітика даних та Інтернет речей стають ключовими елементами, що забезпечують покращену автоматизацію, безпеку та доступність громадянам [43]. У свою чергу, глобальні ініціативи спрямовані на залучення громадян у формування та вдосконалення електронного урядування. Механізми збору зворотного зв'язку, публічні консультації та участь громадських організацій визначають новий рівень взаємодії між владою та громадянами.

Залучення громадськості у процес розробки та впровадження СЕУ є

важливою складовою частиною електронного урядування. Україна, як і багато інших країн, здійснює залучення громадськості до процесу розробки та впровадження СЕУ. Зокрема, в Україні існує законодавство, яке передбачає залучення громадськості до процесу розробки та впровадження СЕУ [43].

Залучення громадськості до процесу розробки та впровадження СЕУ може здійснюватися за допомогою різних методів, таких як громадські слухання, зустрічі з депутатами та посадовцями місцевого самоврядування [44]. Для забезпечення ефективного залучення громадськості до процесу розробки та впровадження СЕУ, в Україні були розроблені Стратегічні Пріоритети залучення громадянського суспільства в процес прийняття рішень. Ці пріоритети були розроблені багатосторонньою групою та подані для обговорення на круглому столі 8 грудня 2014 року у м. Київ для розгляду та рекомендацій щодо наступних дій. Після досягнення консенсусу між усіма зацікавленими сторонами, Рада Європи представить українським органам влади "Стратегічні пріоритети залучення громадянського суспільства в процес прийняття рішень" для їх можливого включення в План Дій Ради Європи для України на 2015-2017 років [44].

Всі зазначені елементи містять компоненти функціональних можливостей організації систем електронного урядування, що є важким, насиченим та структурованим процесом. Значне поліпшення роботи органів державної і публічної влади може принести автоматизація адміністративних процесів через використання систем електронного урядування. За допомогою СЕУ можна автоматизувати багато адміністративних процесів, таких як подача заявок, отримання дозволів, реєстрація бізнесу та інші.

За результатами досліджень, автоматизація адміністративних процесів може призвести до зменшення часу, необхідного для вирішення різноманітних питань, а також до зменшення кількості помилок, пов'язаних з ручним введенням даних [45].

Однак, автоматизація адміністративних процесів також може мати свої недоліки. Наприклад, вона може призвести до зменшення кількості робочих місць, пов'язаних з виконанням адміністративних процесів, а також до зменшення кількості контактів між державними органами та громадянами, що може призвести до зменшення якості надання державних послуг [45].

Електронне урядування стало стратегічним напрямком у зусиллях урядів багатьох країн світу. За останні роки все більше та більше урядів впроваджує та запроваджує системи електронного урядування як засіб зниження витрат, покращення послуг, економії часу, підвищення результативності та ефективності в державному секторі. Електронне урядування та Інтернет внесли суттєві зміни в структуру суспільства, цінності, культуру та способи ведення бізнесу за допомогою реалізації потенціалу інформаційно-комунікаційних технологій (ІКТ) у щоденній роботі [46].

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. Однак це також закликає переглянути шляхи діяльності уряду, функції якого виконуються сьогодні, для покращення процесів та інтеграції.

Уряди обирають різні стратегії для створення електронного уряду. Деякі створюють комплексні довгострокові плани, інші визначають лише кілька ключових сфер як фокус для ранніх проектів. У всіх випадках країни, визначені як найуспішніші, почали з менших проектів, етапно будуючи конструкцію. Дослідники електронного урядування поділяють процес впровадження на фази чи етапи. У цій статті представлені різні дослідження впровадження електронного урядування, що проілюструють переваги впровадження систем електронного уряду та найважливіші проблеми, які впливають на імплементацію та функціонування систем електронного урядування [46].

Тут важливо ввести термін "е-готовність" (електронна готовність), який визначається як здатність країни використовувати "інформаційні та комунікаційні технології (ІКТ) для розвитку своєї економіки і сприяння добробуту" [4]. Крім того, готовність, визначена як "міра якості інформаційної та комунікаційної технології (ІКТ) інфраструктури та здатності її споживачів, підприємств і урядів використовувати ІКТ для своєї користі" [45].

Так, індекси е-готовності визначаються як інструменти для оцінки готовності країн до впровадження електронного урядування та використання інформаційно-комунікаційних технологій (ІКТ) для соціального та економічного розвитку. Ці індекси зазвичай враховують різні аспекти, такі як якість ІКТ інфраструктури, доступність та використання ІКТ громадянами та урядом, інтернет-приєднаність, та інші фактори.

Наприклад, Індекс електронного урядування ООН визначається на основі кількох критеріїв, таких як інтернет-приєднаність, доступність громадян до онлайн-послуг, та використання соціальних мереж. Світовий банк, зокрема, також публікує індекс е-готовності, який оцінює рівень розвитку електронного урядування у різних країнах [46].

Ці індекси допомагають країнам спостерігати за своїм прогресом у впровадженні електронного урядування та визначенні областей для подальших поліпшень. Оцінка готовності до е-урядування є важливою для ефективного використання сучасних технологій у сфері управління та надання послуг громадянам [45].

Існує п'ятиетапний підхід для оцінки прогресу електронного урядування, який відображає еволюцію державних інтернет-ресурсів від початкового етапу до повного інтегрованого електронного урядування. Дозвольте розглянути кожен етап більш детально:

Етап 1: Поява. На початковому етапі уряд формує базову онлайн-присутність через кілька незалежних офіційних веб-сайтів. Інформація є

обмеженою, простою і статичною.

Етап 2: Покращення. Сайти державних органів збільшуються, інформація стає більш динамічною. Зміст та інформація оновлюються з більшою регулярністю.

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 [45].

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 [47].

Етап 2: Взаємодія. На цьому етапі з'являється можливість взаємодії між урядами та громадянами, урядом та бізнесом, або між урядовими установами та державними установами. Веб-сайти на цьому етапі надають контакти електронною поштою та інтерактивні форми для отримання інформації.

Етап 3: Транзакція. На етапі транзакцій користувачі можуть виконувати різні транзакції онлайн, такі як сплата податків, ліцензій або подання пропозицій для закупівель [47].

Етап 4: Трансформація. Це найвищий етап, де відбувається переосмислення організаційних функцій уряду та концепції управління. Трансформація охоплює стратегічні зміни та використання електронних технологій для переформатування способів надання послуг та взаємодії з громадянами та бізнесом [47].

Важливою є ідея того, що перехід від одного етапу до іншого відбувається етапно, і кожен наступний етап включає покращення та розширення функціоналу. Ця модель дозволяє урядам визначати свій поточний рівень електронного урядування та розробляти стратегії для досягнення більш високих ступенів інтеграції та взаємодії з громадянами та бізнесом [47].

Програми електронного уряду дозволяють людям, підприємствам і урядовим секторам отримувати доступ до урядової інформації 24 години на добу, 7 днів на тиждень, що покращує якість цих послуг [48].

Впровадження електронного уряду зменшить вартість і рівень організаційних процесів, шляхом оптимізації та реорганізації операційних процедур [48]. Використання систем електронного уряду покращить ефективність роботи державних установ і надасть державні послуги ефективно та результативно для всіх клієнтів [47].

Електронне урядування має значні переваги щодо економії та покращення роботи державних послуг, включаючи підвищення ефективності, зменшення транзакційних витрат, підвищення прозорості та розширення набору послуг для громадян. 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 [47].

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.
- Допомога у зміцненні довіри між урядами і громадянами, що є важливим фактором належного управління за допомогою інтернет-стратегій, які залучають громадян до політичного процесу та ілюструють прозорість уряду і відповідальність [48].

Підсумовуючи, впровадження електронного уряду не лише економить ресурси, зусилля і гроші, але також може значно підвищити рівень якості обслуговування та скоротити час перебування в державних установах.

Існують кілька проблем і перешкод, які можуть затримати розвиток електронного урядування при його впровадженні. Різноманітність і складність ініціатив електронного уряду передбачають існування широкого спектру проблем і перешкод у його впровадженні та управлінні. Нижче наведено короткий огляд найважливіших та спільних викликів та бар'єрів на основі літературного огляду, як показано в 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 надає огляд основних бар'єрів, які можуть виникнути в процесі впровадження електронного урядування, розподілених за різними категоріями. Впровадження електронного урядування стикається зі значними технологічними викликами, такими як відсутність єдиної стандартизації та сумісної інфраструктури між різними департаментами та агенціями. Додатково, забезпечення конфіденційності та безпеки виявляється критичними бар'єрами для впровадження електронного уряду в інтересах громадян. Забезпечення правових гарантій від уряду буде недостатнім, якщо це не супроводжується технічними рішеннями, прозорими процедурами і, можливо, незалежним аудитом [50].

Відсутність або недоліки в інфраструктурі ІКТ є однією з ключових труднощів у впровадженні електронного урядування. Для успішного переходу до

електронного урядування потрібні архітектурні рішення, які включають набір принципів, моделей і стандартів. Багато розвиваючихся країн стикаються з цифровим розривом, що визначається розривом у доступі до Інтернету між тими, хто має і хто не має цього доступу [50]. Цей розрив ускладнює впровадження електронного уряду в країнах з низьким рівнем доходу, де доступ до технологій обмежений.

Конфіденційність становить критичну проблему як у впровадженні електронного уряду в розвинених країнах, так і в країнах, що розвиваються. Забезпечення належного рівня захисту інформації для фізичних осіб є ключовим аспектом конфіденційності [50]. Електронний уряд повинен ретельно підходити до захисту особистої приватності, технічно та політично вирішуючи питання конфіденційності в контексті електронного уряду.

Складність захисту особистої приватності може утруднити успішне впровадження електронного урядування. Проблеми конфіденційності в електронних мережах потребують ефективних відповідей для збільшення впевненості громадян у використанні електронних урядових послуг. Забезпечення довіри громадян в конфіденційність та обережне ставлення до їх особистої інформації є ключовими для успішного впровадження програм електронного урядування.

Конфіденційність та захист особистих даних повинні залишатися пріоритетами при розробці та утриманні веб-сайтів, що забезпечують безпечний збір даних. Планування та розробка систем електронного урядування повинні враховувати конфіденційність, оскільки вставити захист важко після побудови електронної системи. Комплексна політика конфіденційності повинна чітко визначати права громадян на конфіденційність та зобов'язати зберігати особисті дані лише для законних цілей [49, 49]. У зв'язку зі збором та управлінням великою кількістю громадянських даних, важливо враховувати їхню конфіденційність та забезпечувати безпеку отриманих даних. Також слід враховувати різні правові та

культурні відмінності в розумінні приватності в різних країнах [49].

Важливо враховувати, що інфраструктура ІКТ не обмежується лише телекомунікаціями та комп'ютерами. Для успішного використання програм електронного урядування необхідна електронна готовність та ІКТ-грамотність. Освіта та доступ до інформації відіграють важливу роль у забезпеченні ефективності електронного урядування. Розвиток освіти та співпраця з приватним сектором можуть сприяти встановленню сучасної інфраструктури, яка забезпечить доступ до можливостей для всіх груп населення та осіб. Отже, вирішення викликів інфраструктури займається не лише технічними аспектами, але й важливими аспектами освіти та співпраці.

Впровадження електронного урядування представляє собою не лише технічний виклик, але, передусім, організаційний. Організаційні аспекти включають такі виклики, як підтримка вищого керівництва, стійкість до змін у впровадженні електронних процесів, необхідність сприяння співпраці та недостатній кваліфікований персонал разом із необхідністю навчання [49].

- Підтримка вищого керівництва: Забезпечення підтримки та залучення вищого керівництва є ключовим елементом успішного впровадження електронного урядування. Високий рівень підтримки дозволяє виділити необхідні ресурси та забезпечити стратегічне керівництво проектом.

- 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: Ефективне співробітництво між різними відділами та агентствами влади може бути викликом. Крім того, брак кваліфікованого персоналу може ускладнити ефективне впровадження електронних ініціатив.

- 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 [48].

Соціальні питання, пов'язані з електронним урядуванням, переважно стосуються можливості використання широким колом людей. Це передбачає створення інтерфейсу, який буде доступним для всіх користувачів урядових послуг. Серед соціальних викликів можна виділити кілька факторів, таких як цифровий розрив, культурні різниці, рівень освіти та доходи. У цьому контексті розглянемо два з перерахованих факторів: цифровий розрив та культурні особливості.

- Цифровий розрив: Один із ключових викликів у впровадженні електронного урядування - це цифровий розрив між тими, хто має доступ до Інтернету та цифрових технологій, і тими, хто не має. Різниця в доступі може призвести до виникнення соціальних нерівностей та обмежити можливість отримання користі від електронних урядових послуг для частини населення.

- Культурні особливості: Різниці в культурних підходах та очікуваннях можуть стати викликом для впровадження 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]

Підбиваючи підсумок, у цьому підрозділі висвітлені різні етапи впровадження електронного урядування, наголошені переваги та перешкоди, які можуть виникнути на шляху до успіху впровадження системи електронного урядування. Зрозуміло, що електронний уряд передбачає кілька стадій або фаз розвитку і може принести багато переваг для всіх секторів влади, громадян та бізнесу. Однак впровадження електронного уряду не є простим завданням і стикається з численними проблемами та бар'єрами, які вимагають уважного

вивчення та вирішення.

2.2. Роль інформаційних систем управління в оптимізації процесів публічного адміністрування.

Ефективність функціонування системи публічного управління та адміністрування проявляється у практичному втіленні прийнятих рішень у різних галузях економіки, соціальної сфери та екології. Це є базовим принципом в узгодженій реформі системи державного управління, спрямованій на підвищення ефективності діяльності владних структур як у стратегічному, так і в операційному вимірах.

Проте важливо визначати та оцінювати цю ефективність на основі конкретних та практично застосовних критеріїв. На жаль, в сучасний період часу відсутній загальноприйнятий підхід до визначення та вимірювання ефективності в контексті діяльності органів влади. Також не існує стандартних методик чи організаційних процедур для проведення об'єктивного оцінювання.

У цьому контексті розробка надійних критеріїв та методик, які враховують практичні потреби, стає ключовим завданням. Необхідно розглядати і впроваджувати нові підходи до оцінювання ефективності системи публічного управління, забезпечуючи об'єктивні та корисні результати для подальших стратегічних та операційних рішень.

У теорії існують різноманітні підходи до оцінювання ефективності управління, включаючи цільовий, функціональний, композиційний, поведінковий та інші. З урахуванням практичної специфіки управлінської діяльності в галузі публічного управління та адміністрування, одним з найбільш відповідних підходів, розглянутих у наукових дослідженнях, є цільовий підхід.

Цей підхід базується на ідеї, що основною метою будь-якої системи управління у цих сферах є досягнення встановлених цілей найбільш

раціональним способом. Цей цільовий підхід часто поєднується з методами оцінювання ефективності, що ґрунтуються на поведінковому підході, процедури якого базуються на вимірах досягнення балансу інтересів всіх зацікавлених груп у результатах діяльності публічних інститутів [50].

Цей критерій розглядається як основний у процесах оцінювання ефективності державного управління і використовується системою показників для визначення ступеня досягнення поставлених цілей. Для цього використовуються як методи прямих розрахунків, так і методи опосередкованого оцінювання, такі як експертні методи, анкетування та інших [50].

Інтеграція інформаційних систем управління в оптимізації процесів публічного адміністрування відіграє ключову роль у поліпшенні ефективності та якості надання громадських послуг [51]. Основні аспекти цієї інтеграції включають:

- 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: Інтеграція різних інформаційних систем дозволяє централізовано зберігати та обробляти дані. Це полегшує доступ до інформації для різних рівнів влади, сприяючи швидкому та точному прийняттю рішень.
- Підвищення координації та взаємодії: Інтеграція систем управління сприяє покращенню внутрішнього та міжсекторного обміну інформацією. Це дозволяє різним гілкам та рівням влади ефективно співпрацювати для вирішення загальних завдань та досягнення стратегічних цілей.
- Забезпечення прозорості та відкритості: Інтеграція систем дозволяє створити єдиний простір для обміну інформацією між владними органами та громадянами. Це сприяє збільшенню прозорості владних рішень та стимулює

взаємодію між владою та громадськістю.

- Підвищення безпеки даних: Інтеграція відповідних систем дозволяє ефективно керувати та захищати конфіденційну інформацію. Це важливо для забезпечення високого рівня безпеки та дотримання нормативних вимог [51].

Повернемося до ключового поняття - інформаційна система (ІС) - це комплекс заходів для обробки інформації з відповідними організаційними ресурсами, такими як людські, технічні та фінансові, які надають та поширюють інформацію. Зв'язки між об'єктами та взаємодія системи із середовищем реалізуються шляхом обміну інформацією. Кожна інформаційна система включає базу даних та набір програм, які надають різні класи користувачів доступ до даних цієї бази, дозволяючи їм виконувати щоденні завдання. На основі цього, інформаційну систему можна визначити як сукупність прийомів, технологій, методів та процедур для збору, планування, підготовки, передачі, зберігання та обробки даних, а також поширення та представлення інформації для прийняття рішень [52].

Інтенсивний розвиток інформаційних систем розпочинається з впровадження ЕОМ та іншого обладнання для обробки бізнес-інформації, яка раніше виконувалася вручну. Розвиток інформаційних систем має свою основу, межі та мотивації; сьогодні теорія систем та інформатика виступають як основа, з якої виводяться концепції розробки інформаційних систем. Інформаційні системи, які використовують комп'ютери та інформаційні технології (ІТ) у цій галузі, називаються комп'ютерними інформаційними системами (СВІС). Завдання інформаційної системи - перетворити вхідну інформацію на вихідну інформацію, корисну для прийняття рішень [51].

Зворотній зв'язок відіграє роль у контролі за тим, чи відповідає результат реальному значенню. Якщо реальне значення не збігається з очікуваним вихідним, проводиться перевірка та корекція вхідних даних. Помилки, що часто виникають при введенні даних в комп'ютер, можуть бути результатом

неуважності або втоми людини і легко виправляються. Помилки в програмі, з іншого боку, можуть мати більш глибокі причини через складність програми, яка може бути настільки великою, що програміст практично не може контролювати всю програму. Навіть коли очевидно, що десь у програмі виникла помилка, визначити її місце та виправити стає надзвичайно важко. Після виявлення та виправлення помилки існує значна ймовірність того, що це може вплинути на виконання інших частин програми, навіть до такої міри, що нова помилка може бути критичною для виконання інших функцій програми. Вирішення труднощів, які виникають через складність програм, полягає в створенні структури, зрозумілої для програміста (застосування структурного програмування під час розробки програми). Програма повинна бути структурована на модулі, які є відносно незалежними, дозволяючи обробку їх окремо, незалежно від інших (застосування модульного програмування під час розробки програми) [52].

Однією з ключових складових кожного "перехідного пакету" є реформа державного управління. Ця реформа є надзвичайно важливою, але водночас дуже складною у впровадженні. Це підтверджено досвідом Сербії. У кінці 2003 року Сербське Агентство розвитку державного управління звернулося до державної компанії Statskonsult з Норвегії з проханням підготувати доповідь щодо реформи державного управління в Сербії. Норвезьке Міністерство закордонних справ схвалило фінансування цього дослідження, яке складається з п'яти розділів: "Що передувало реформі - спадок і виклики", "Опис реформи - досягнення та невдачі", "Оцінка реформи", "Пояснення реформи", "Адаптація реформи". Невід'ємною частиною дослідження є чотири детальні додатки [53, с. 54].

Були проаналізовані три тісно пов'язаних питання: наскільки вдалося реалізувати громадську адміністративну реформу в Сербії протягом 2001–2004 рр. (до березня 2004 р., коли було сформовано новий уряд); що стимулювало та що перешкоджало цій реформі; чи слід коригувати програму реформ та процес реформ, і якщо так, то як це зробити? 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 аналізі автори зосередилися на трьох змінних, які мають ключове значення в літературі про інституційні зміни в Центральній та Східній Європі. Ті змінні - "структура" (фактична інституційна спроможність, доступна державним лідерам), "лідерство" і "зовнішні фактори", використовувалися для оцінки результатів реформи державного управління в Сербії на основі двох джерел даних: оцінок тих, хто був безпосередньо залучений до реформи або спостерігав за нею, а також порівняння прогресу в розвитку загального адміністративного потенціалу Сербії з Словенією, Хорватією та Македонією [54].

Результати реформи державного управління в Сербії можна визнати обмеженими. Автори вбачають, що ключовим досягненням в цей період є значна заміна кадрів. Однак виникли деякі проблеми. Протягом трьох років конституційна система стала комплексною, а межа між правом і політикою стала нечіткою. Додатково, сербські міністерства можна охарактеризувати як централізовану бюрократію, з фокусом на контролі та прийнятті рішень зверху донизу. Керівництво та структура створили проблеми та обмеження для реформаторських зусиль. Лідерство мало негативний вплив через свою фрагментарність і відволікання уваги та енергії на інші питання. Конструкція була недостатньою для створення потенціалу для координації, співпраці, комунікації та розвитку політики. Зовнішні фактори, зокрема донорська допомога, частіше позитивно впливали на адміністративні зміни, але це було необхідною, але недостатньою умовою для створення нових можливостей. Заключний висновок доповіді полягає в тому, що державна система Сербії є слабкою, з недостатньою міжвідомчою координацією, тому необхідно вдосконалювати координацію та комунікацію через тонко узгоджені заходи, щоб

досягти поліпшень у інноваціях та розвитку публічної політики [53, 54].

Термін “інформаційна система” використовується в різних контекстах та може мати різні визначення. Згідно з положенням “Про інформаційну систему управління людськими ресурсами в державних органах”, прийнятим рішенням кабінету міністрів від 28 грудня 2020 року, інформаційна система визначається як автоматизована система для збору, обробки, зберігання та захисту інформації про працівників органів впровадження. Ця система створюється та використовується відповідно до визначених законодавством правил для забезпечення функціонування централізованої бази даних працівників органів впровадження, а також для автоматизації та цифровізації процесів управління персоналом та обліку заробітної плати. Сам документ встановлює порядок функціонування інформаційної системи управління людськими ресурсами в державних органах як автоматизованої системи для збирання, обробки, зберігання та захисту інформації в сфері державної служби [55].

В контексті публічного і державного адміністрування система працює для забезпечення наступних цілей:

- Створення єдиної бази даних державних службовців та інших працівників органів впровадження [55].
- Автоматизація та цифровізація процесів управління людськими ресурсами в органах впровадження та прийняття рішень з кадрових питань.
- Моніторинг результативності діяльності органів впровадження в галузі управління персоналом.
- Забезпечення відкритості та прозорості інформації про людські ресурси та оплату праці в органах впровадження.
- Посилення спроможності структурних підрозділів управління персоналом та бухгалтерського обліку в органах впровадження.
- Розвиток сучасного управління людськими ресурсами через оперативність, достовірність, повноту, доступність, багатоваріантність та

надійність обліку, обробки, накопичення, передачі та представлення інформації в сфері державної служби [55].

- Функціонування інформаційної системи на державній службі та електронна взаємодія державних електронних інформаційних ресурсів в частині управління людськими ресурсами.

- Електронна взаємодія між органами впровадження.

- Надання доступу працівникам органів впровадження до інформації через електронний кабінет користувача інформаційної системи для електронної взаємодії із структурними підрозділами та іншими працівниками органу впровадження [55].

Розуміючи, що інформаційні системи управління вже визначені в чинному законодавстві, важливо підкреслити їхню роль у забезпеченні ефективності та оптимізації процесів у публічному та державному секторі. Зокрема, вказівка на те, що додаткові нормативно-правові акти не є необхідними, може бути ключовою для розуміння та впровадження цих інформаційних систем.

Сучасна система управління, яка активно впроваджується Київською міською радою та міською державною адміністрацією, має на меті оптимізацію процесів у структурі публічного та державного менеджменту. Розвиток суспільства вимагає використання технологічних рішень для спрощення процесів у всіх галузях, особливо в умовах пандемії, яка змусила змінити формат роботи органів державної влади та місцевого самоврядування, спрямовуючи їх на онлайн-функціонування.

Київська міська рада, представник органів місцевого самоврядування, активно використовує технологічні інновації для забезпечення ефективної роботи. Дев'яте скликання ради систематично використовує онлайн-формат, здійснюючи технологічне голосування під час пленарних засідань та використовуючи електронно-цифровий підпис. З метою поліпшення роботи міської ради було розроблено спеціальний додаток.

Київська міська державна адміністрація, реагуючи на локдаун, перейшла до онлайн-режиму, де більшість працівників працювала віддалено. За допомогою електронних систем документообігу, які були впроваджені ще до початку пандемії, орган місцевого управління забезпечив безперебійну роботу та здійснив перехід до сучасних форм організації робочих процесів. Ці процеси є актуальними і в умовах оборони від російської агресії.

Проте, важливою складовою сучасного управління є не лише організаційні аспекти, але й сутність діяльності. На сьогоднішній день Київська міська державна адміністрація активно використовує електронне управління для оптимізації міського простору. Основний інструмент цього процесу - Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради. Цей департамент визначає потребу у створенні електронних інформаційних ресурсів і баз даних для створення єдиного інформаційного простору територіальної громади [50].

Зокрема, йому доручено організацію формування, розвитку, супроводження та забезпечення інформаційної безпеки електронних інформаційних ресурсів і баз даних. Також він координує та здійснює методичне забезпечення діяльності органів державної влади та органів місцевого самоврядування у м. Києві, а також підприємств, установ та організацій у сфері інформатизації, телекомунікаційних систем та технологій, електронного урядування, захисту інформації та інших важливих напрямків [50].

Законодавство України не лише схвалює, але й активно спонукає державні установи, органи публічного адміністрування, а також бізнес прискорюватися у впровадженні інформаційних технологій. Це визначається на законодавчому рівні та через впровадження різноманітних тематичних програм. Зокрема, Закон України "Про Національну програму інформатизації", прийнятий наприкінці 2022 року, визначає національну програму інформатизації як комплекс завдань, програм, проектів та робіт з інформатизації [56]. Ці заходи спрямовані на

розвиток інформаційного суспільства шляхом концентрації та раціонального використання фінансових, матеріально-технічних та інших ресурсів, виробничого і науково-технічного потенціалу держави. Програма передбачає координацію діяльності державних органів, органів місцевого самоврядування, а також підприємств, установ і організацій, незалежно від форми власності [56].

Національна програма інформатизації у своїх завданнях і відтворює основну роль інформаційних систем управління в оптимізації процесів як державного так і публічного управління. Вона спрямована на забезпечення:

- розробки, впровадження та застосування інформаційно-комунікаційних технологій у державному управлінні, місцевому самоврядуванні та суспільному житті;
- реалізації та впровадження заходів, спрямованих на розвиток електронного урядування та електронної демократії;
- створення та розвитку системи державних інформаційних ресурсів;
- рівного доступу до інформаційно-комунікаційних технологій та підвищення рівня освіченості громадян з питань інформаційно-комунікаційних технологій;
- удосконалення процедури надання публічних (електронних публічних) послуг;
- організації інформаційної взаємодії державних органів та органів місцевого самоврядування за допомогою електронного документообігу;
- створення систем інформаційної та аналітичної підтримки діяльності державних органів та органів місцевого самоврядування;
- підвищення ефективності вітчизняного виробництва шляхом використання інформаційно-комунікаційних та цифрових технологій [56];

Для підвищення ефективності роботи органів місцевого самоврядування важливо активно впроваджувати інформаційні технології. Однак існують ряд проблем, які гальмують розвиток цього напрямку, зокрема:

- Недостатня кількість та якість комп'ютерної техніки: У багатьох містах і селах України проблемою залишається недостатнє обладнання для фахівців, яке відповідало б сучасним вимогам технологій.

- Неадекватність обладнання до обсягів роботи: Використання непридатної техніки призводить до її швидкого виходу із ладу, при відсутності резервної техніки працювати стає складніше.

- Низький рівень навичок робітників: Відсутність необхідних навичок у роботі з програмним комплексом стає перешкодою для виконання роботи.

- Відсутність українського перекладу: Брак перекладу для іншомовних програм створює лінгвістичний бар'єр, що негативно впливає на ефективність роботи.

- Брак фінансування є ключовою проблемою для інформаційно-комунікаційного розвитку органів місцевого самоврядування [50].

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.

- Освітні заходи: Проведення навчань серед державних службовців та осіб місцевого самоврядування щодо сучасних інформаційних технологій для поліпшення їхнього рівня обізнаності.

- Впровадження електронних систем документообігу: Запровадження таких систем сприяє швидкому вирішенню питань місцевого значення, раціональному використанню місцевого бюджету та систематизації документів в органах місцевого самоврядування [50].

Незважаючи на виклики, які виникають у процесі імплементації інформаційних технологій, їхня користь для органів місцевого самоврядування та підвищення рівня сервісу для громадян є невідомою. Ретельне врахування цих

аспектів дозволить забезпечити ефективне та інноваційне управління на місцевому рівні.

Висновки за розділом 2.

У розділі стратегічно досліджено інтеграцію інформаційних технологій у сферу публічного адміністрування, проведено аналіз в деталях систем електронного урядування: формування, організація та функціональні можливості та роль інформаційних систем управління в оптимізації процесів публічного адміністрування.

В рамках дослідження, присвяченого системам електронного урядування, відзначається, що побудова та управління цими системами визначають стратегічний напрямок для розбудови взаємодії між владою та громадянами. Відзначається, що це створення має величезне стратегічне значення у розвитку прозорих та доступних адміністративних процесів. Функціональні можливості цих систем розглядаються як необхідні для автоматизації та поліпшення роботи державних структур, що сприяє оптимізації їх функціонування.

Дослідження ролі інформаційних систем управління надало можливість виявити, що впровадження цих систем є стратегічно необхідним етапом для підвищення ефективності та координації в адмініструванні. Зазначається, що ці інформаційні системи дозволяють не тільки ефективно використовувати та аналізувати дані, але і спрощують процеси прийняття рішень, забезпечуючи високий рівень оперативності. Впровадження цих систем вважається суттєвим для створення гнучких та адаптивних систем управління, що відповідають вимогам сучасного суспільства.

Загалом підкреслюється важливість інформаційних технологій у публічному адмініструванні, визначаючи їхній потенціал для трансформації управлінських підходів та досягнення високої ефективності та взаємодії між

урядом та громадянами.

РОЗДІЛ 3. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ІНТЕНСИВНОГО ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

3.1. Загрози та ризики інформаційної безпеки в публічному секторі.

Не є новиною, що інформація у сучасному світі стала ключовим ресурсом, а питання інформаційної безпеки в публічному секторі стає надзвичайно важливим. Зростання обсягу електронної обробки даних та використання інформаційних технологій у державному управлінні призводять до зростання загроз та ризиків, що можуть впливати на ефективність та безпеку урядових органів. Відповідно, розуміння та аналіз загроз і ризиків інформаційної безпеки стає необхідністю для забезпечення надійності та стійкості публічного сектору перед сучасними викликами кіберпростору. У цьому контексті важливо розглядати це питання як ключовий аспект стратегічного управління інформаційними ресурсами та забезпеченням безпеки в умовах сучасного цифрового середовища.

Інформаційна безпека в публічному секторі - це комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, що обробляється і зберігається в системах публічного управління.

Президент України Володимир Зеленський увів в дію рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року “Про Стратегію інформаційної безпеки”. Ця стратегія визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [57].

Основною загрозою для інформаційної безпеки у публічному секторі є кібератаки. За даними CERT-UA, лише за перший квартал 2023 року кількість

кіберзлочинності в Україні зросла на 65%, що свідчить про актуальність проблеми [58]. Зріст кіберзлочинності також пов'язаний із нездоровим інтересом з боку хакерів держави-агресора. Насамперед це проявляється в атаках на інформаційні системи силових та урядових структур, а також у постійних проявах несанкціонованого втручання в роботу систем електрозв'язку та об'єктів критичної інфраструктури держави.

На підставі вищевикладеного необхідно розглядати інформаційну безпеку не тільки як технічний аспект, але й як складну систему, що включає в себе ефективні правові, організаційні та технічні заходи. Важливість введення цих заходів підкреслюється в контексті постійного розвитку технологій та зростання кількості кіберзагроз [58].

Інформаційна безпека в публічному секторі – це комплексний підхід до захисту інформації від різноманітних загроз та забезпечення безперебійного функціонування державних структур. Ефективне вирішення цього завдання вимагає поєднання законодавчих ініціатив, сучасних технологій та освітніх заходів для забезпечення високого рівня інформаційної безпеки та збереження довіри громадян до уряду.

Урядові органи та органи місцевого самоврядування відіграють ключову роль у забезпеченні функціонування суспільства, і їхні функції все більше залежать від інформаційних технологій та обробки даних. Розширення цифрових можливостей уряду та місцевої влади, таких як електронне урядування, облік даних громадян та державних справ, а також онлайн-сервіси, роблять інформаційний ресурс надзвичайно важливим. Однак захист інформації в урядових та місцевих органах має вирішальне значення для забезпечення конфіденційності, цілісності та доступності даних. Конфіденційність забезпечує захист від несанкціонованого доступу до чутливої інформації, такої як особисті дані громадян чи стратегічні плани. Цілісність важлива для гарантування, що дані не піддаються невідомим змінам чи руйнації, забезпечуючи достовірність

інформації. А доступність стає критичною для забезпечення безперебійної роботи урядових служб та гарантування доступу до необхідної інформації в будь-який момент.

Потреба в ефективному захисті інформації обумовлена не лише внутрішніми потребами держави, але й зобов'язаннями перед громадянами. Державні структури володіють величезним обсягом особистих даних та конфіденційної інформації, тому їм доручено важливу місію її надійного збереження. Збій у цьому питанні може призвести не лише до технічних проблем, але й до порушення довіри громадськості, що може суттєво вплинути на владні структури та їхню легітимність [59].

Важливо зазначити, що в реаліях війни, інформація, що містить таємні дані, визначає ключові дії від загального перебігу подій як на міжнародній політичній арені, так і безпосередньо на полі бою. Численні значущі успішні операції спецслужб України, спрямовані на перемогу ворога, були б неможливі без належного дотримання норм зберігання та передачі інформації як всередині відомств, так і поза його межами.

Розглянемо основні загрози для інформаційної безпеки в публічному секторі [60].

1. 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:

- Розповсюдження вірусів, троянців, черв'яків та інших шкідливих програм: для отримання несанкціонованого доступу або завдання шкоди.
- Кібершпигунство: використання програм для збору конфіденційної інформації, такої як паролі, ключі безпеки тощо; активності, спрямовані на нелегальне отримання інформації з комп'ютерних систем та мереж.
- Кібертероризм: використання великої кількості запитань для перевантаження серверів та забруднення доступу до ресурсів (DDos атаки); спроби атак на електроенергетичні системи, транспортні мережі тощо.
- Соціальний інжиніринг: використання підроблених повідомлень або веб-сайтів для отримання конфіденційної інформації (фішинг); використання психологічних методів для отримання доступу до інформації.
- Кібервійна: використання кіберзасобів у воєнний час для збору інформації та завдання шкоди ворожим інформаційним системам.
- 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 [60, 61].

Також хотілося б додати новий вид кібератак, який став можливим завдяки відкритості та публічності даних з Інтернету. Психологічні операції (ІПСО) — це операції, спрямовані на донесення обраної інформації та індикаторів до аудиторії з метою впливу на її мотивації, об'єктивні міркування і, в кінцевому підсумку, на поведінку урядів, організацій, груп та великих іноземних держав [62].

Цей вид кібератак використовує психологічні методи для формування перцепції, уподобань та взаємин між різними суб'єктами у Інтернеті. ІПСО може включати в себе розповсюдження дезінформації, маніпулювання соціальними мережами, створення фейкових ідентичностей та інші техніки для створення враження або впливу на думку громадськості.

Вплив кібератак на державні інформаційні системи:

- **Порушення конфіденційності:** Кібератаки можуть викликати витік конфіденційної інформації, порушуючи та піддаючи ризику надійність 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 невірної прийняття рішень на рівні влади [62].

Наприкінці квітня 2022 року, виходячи з опублікованого звіту підрозділу з кібербезпеки компанії Microsoft (Digital Security Unit), розкрито подробиці щодо російської кіберактивності в ході широкомасштабної агресії проти України [63]. Цей звіт виник в результаті співпраці Microsoft з представниками українських державних установ з кібербезпеки та приватного сектору України [63].

Згідно з опублікованим документом, діяльність російських хакерів переважно була спрямована на компрометацію об'єктів по всій території України. Ці дії включали дві основні фази: спершу проводились фішингові атаки для отримання доступу до внутрішніх систем цілей, а потім акцентували увагу на знищенні або модифікації даних, а також здійснювали кібершпигунські операції [63].

У період з 23 лютого по 8 квітня 2022 року було зафіксовано щонайменше 40 успішних кібератак, які призвели до пошкодження файлів в сотнях систем десятків українських організацій. Використано мінімум 8 різних сімейств вірусів для перезаписування та видалення даних, виведення з ладу комп'ютерів та впливу на системи управління промисловими процесами (ICS). 40% деструктивних атак були спрямовані на об'єкти критичної інфраструктури (ОКІ), що може негативно впливати на уряд, військову сферу, економіку та громадян. 32% інцидентів стосувались українських державних установ на різних рівнях [63].

Microsoft ідентифікувала групи хакерів, пов'язані з ключовими безпековими структурами Росії: ФСБ, ГУ ГШ ЗС РФ та СЗР РФ. Російські хакери готувалися до військової агресії проти України не менше з березня 2021 року, що включало фішингові кампанії та спроби проведення кібератак через ланцюжок постачання.

Звіт також підкреслює адаптивність російських хакерів, які швидко модифікують віруси для ускладнення їх виявлення. З розвитком конфлікту, ймовірність виявлення руйнівного шкідливого програмного забезпечення зростає. Зазначено, що зловмисники, здатні підтримувати високий темп адаптації, можуть представляти значну загрозу, а їхні дії можуть стати ще більш деструктивними [63].

За висновками звіту, з розвитком конфлікту можна очікувати використання резервних можливостей, таких як вразливості "нульового дня", атаки на об'єкти критичної інфраструктури та кібератаки через ланцюжок постачання. Підвищення ефективності кібердопомоги Україні може викликати використання російськими хакерами вразливостей "нульового дня", що може стати загрозою для організацій у всьому світі [63].

Згідно з документом, передбачається, що ворожа кіберактивність буде фокусуватися на телекомунікаційному секторі України, зокрема, на інтернет-провайдерах. Росія планує розширити сферу кібероперацій і зосередитися на країнах, які надають допомогу Україні. Ці операції охоплюватимуть не лише кібершпигунство, але й кібердиверсії [63].

Звіт також містить перелік типових тактик і методів зловмисної діяльності російських хакерів, а також надає практичні рекомендації командам кібербезпеки для зменшення загроз від деструктивних кібератак. У цьому контексті важливо підкреслити ключову роль у посиленні заходів кіберзахисту та постійному оновленні кібербезпекових стратегій [63].

Загальною тенденцією є те, що конфлікт із застосуванням кіберзброї на

етапі активних воєнних операцій стає неабияким викликом для кібербезпеки, вимагаючи найвищого рівня підготовки та відповідальності від усіх сторін, як державних, так і приватних [63].

2. Витік конфіденційної інформації є серйозною загрозою для урядових органів та громадськості, і може призвести до негативних наслідків для національної безпеки та особистої приватності. Розглянемо форми та методи витоків, наслідки цих витоків та заходи для їхнього запобігання.

Форми та методи витоків конфіденційної інформації, у більшій мірі або опосередковано залежать від дії, що призвели до такого витоку. Насамперед, витік інформації у своїй формі і є продуктом або результатом дій кібератак та кіберзлочинів, зазначених вище [64].

Наслідки для урядових органів та громадськості:

- Втрата довіри: Витік конфіденційної інформації може призвести до втрати довіри до урядових органів та підвищити ризик корупції.
- Загроза національній безпеці: Витік конфіденційної інформації, особливо з області безпеки, може відкрити двері для агресії та терористичних дій.
- Втрата конкурентного переваги: У випадку витоку комерційної інформації, урядові органи можуть втратити конкурентну перевагу в економічних питаннях [64].

Ефективне управління та запобігання витоку конфіденційної інформації вимагає комплексного підходу, що об'єднує технічні, організаційні та освітні заходи. Розуміння потенційних ризиків і прийняття відповідних заходів може допомогти забезпечити стійкість інформаційних систем та захистити конфіденційну інформацію.

Всі напрямки потенційного витоку конфіденційної інформації можна класифікувати як непрямі та прямі. Непрямі канали характеризуються відсутністю необхідності безпосереднього доступу до технічних засобів інформаційної системи. Прямі канали, навпаки, передбачають прямий доступ до

апаратного забезпечення та даних інформаційної системи [65].

Приклади непрямих каналів витоку:

- Крадіжка або втрата носіїв інформації: Один із варіантів цього типу - крадіжка чи втрата фізичних пристроїв, що містять конфіденційну інформацію. Дослідження не знищеного сміття також може призвести до непередбачуваних наслідків.
- Дистанційне фотографування та прослуховування: Використання технік дистанційного фотографування та прослуховування може стати способом для здобуття конфіденційної інформації без прямого доступу.
- Перехоплення електромагнітних випромінювань: Використання спеціальних пристроїв для перехоплення електромагнітних випромінювань може дозволити отримання конфіденційної інформації без прямого втручання в систему [66].

Приклади прямих каналів витоку:

- Інсайдерські дії (людський фактор): Витік інформації через недотримання комерційної таємниці може бути викликаний неправомірними діями власних працівників.
- Пряме копіювання: Фізичне або електронне копіювання конфіденційної інформації може бути виконане з прямим доступом до джерела [66].

Класифікація каналів витоку за фізичними властивостями та принципами функціонування включає такі категорії:

- Акустичні канали: Включають методи запису звуку, підслуховування та прослуховування як засоби отримання інформації.
- Оптичні канали: Використовують візуальні методи, такі як фотографування, відеозйомка та спостереження, для здобуття інформації.
- Електромагнітні канали: Спрямовані на копіювання полів шляхом зняття індуктивних наводок або використання радіовипромінювань.

- Матеріальні канали: Залучають фізичні носії інформації, такі як папір або інші матеріали, для передачі конфіденційної інформації [66].

Аналіз різноманітних каналів витоку конфіденційної інформації враховує різноманітні методи та можливості, які можуть використовувати зловмисники для незаконного отримання секретної інформації. Своєчасне виявлення та запобігання таким витокам стає важливим етапом забезпечення інформаційної безпеки.

Крім того, можна класифікувати канали витоку інформації за їхніми фізичними властивостями та принципами функціонування. Зокрема, технічні канали перехоплення інформації можна розділити на природні та спеціально створені.

Природні канали витоку інформації включають у себе електромагнітні канали витоку інформації, які виникають внаслідок побічних електромагнітних випромінювань під час обробки інформації технічними засобами. Також можливі наведення в лініях електроживлення та інші електромагнітні явища, які можуть викликати непередбачені витoki інформації. Спеціально створені канали витоку інформації включають електронні пристрої перехоплення інформації, такі як закладні пристрої. Вони використовуються для створення каналів витоку, вбудовуючи електронні пристрої у технічний засіб обробки інформації. Ці пристрої можуть бути використані для непомітного перехоплення та передачі інформації. Високочастотне опромінення технічного засобу обробки інформації включає створення спеціальних електромагнітних полів, які можуть викликати непередбачені витoki інформації через електромагнітні випромінювання [66].

Розділення технічних каналів витоку інформації за їхніми характеристиками та методами дозволяє краще розуміти різноманітні загрози, з якими може стикатися публічний сектор. Заходи з протидії таким каналам витоку повинні враховувати різні аспекти та можливості, щоб забезпечити ефективний захист конфіденційної інформації та забезпечити інформаційну безпеку в

урядових органах та громадськості.

У висновку щодо загроз для інформаційної безпеки в публічному секторі можна виділити кілька ключових аспектів. Перше, що варто врахувати, це постійна еволюція кіберзагроз, яка висуває виклики перед урядовими структурами. Кіберзлочинці постійно адаптують свої методи та тактики, використовуючи нові технології та шляхи атак [65].

Другий аспект полягає у важливості застосування комплексного підходу до кібербезпеки в публічному секторі. Це включає в себе не лише технічні заходи, такі як захист мереж та даних, але й вдосконалення кадрового забезпечення, розвиток культури безпеки та постійну підготовку персоналу.

Третій аспект стосується важливості співпраці між урядовими установами, приватним сектором та міжнародними партнерами у сфері кібербезпеки. Обмін інформацією та спільна реакція на кіберзагрози можуть виявитися ключовими факторами у запобіганні та ліквідації кібератак.

Необхідно також акцентувати увагу на вдосконаленні систем виявлення та реагування на інциденти. Розробка та впровадження сучасних засобів моніторингу та аналізу дозволять вчасно виявляти та відсікати потенційні загрози [64].

Узагальнюючи, ефективна кібербезпека в публічному секторі вимагає поєднання технічних заходів, глибокого розуміння кіберзагроз, плідної співпраці та вдосконалення культури безпеки на всіх рівнях. Лише через цей комплексний підхід можна забезпечити надійний захист інформаційних ресурсів та дотримання високих стандартів інформаційної безпеки в публічному секторі.

3.2. Стратегії забезпечення інформаційної безпеки в умовах використання сучасних інформаційних технологій в публічному управлінні.

Одним з ключових факторів, що визначає успіх у сфері інформаційної

безпеки, є їх відкритість до інновацій, робота в перспективних напрямках розвитку та інноваційна активність. Зростаюче використання інформаційних технологій призводить до підвищення ризиків цифрової безпеки. Кіберінциденти призводять до різного роду збитків для компаній. Для вирішення цих завдань існує безліч технічних і програмних продуктів для забезпечення інформаційної безпеки підприємств. Придбання та розробка інноваційних продуктів у сфері інформаційної безпеки дозволяє компаніям побудувати ефективну систему захисту від загроз та забезпечити успішну роботу та довгостроковий розвиток.

Сучасний етап розвитку інформаційних технологій характеризується можливістю масового інформаційного впливу на особистість та громадську свідомість, іноді доходячи до рівня широкомасштабних інформаційних конфліктів. В цьому контексті принцип інформаційної безпеки в системі державного управління став необхідною протиположністю принципу свободи інформації. Ця зміна обумовлена глобальною інформаційною революцією, стрімким розвитком та широким впровадженням новітніх інформаційних технологій та глобальних телекомунікацій.

Європейський досвід розвитку інформаційного ринку в системі громадського управління для сталого розвитку регіону свідчить про необхідність постійного дотримання економічної та соціальної інформації в управлінській-підприємницькій діяльності. Зростаючий вплив та важливість інформаційної складової суспільства, а також психологічні та технічні можливості для маніпулювання масовою свідомістю, вимагають переходу до прогностичної розширеної моделі інформаційної підтримки. Ця модель має забезпечити ефективний захист від інформаційних та технологічних методів психологічного впливу, враховуючи зростаючу потребу суспільства в корисній інформації [67].

В рамках інформаційного забезпечення національної безпеки та захисту особистої інформації важлива боротьба з кіберзлочинністю, особливо актуальною для європейських країн, що відрізняються високим рівнем

комп'ютеризації. Основним міжнародно-правовим документом, який регулює публічні відносини в сфері боротьби з кіберзлочинністю, є Конвенція Ради Європи про кіберзлочинність. Більшість європейських країн прийняли закони, які дозволяють притягувати постачальників до відповідальності за публікацію незаконного вмісту на своїх веб-сайтах. Крім того, деякі правила обмежують доступ провайдерів до джерел інформації. Оператори мереж не несуть відповідальності за зміст інформації, яка передається мережами, але вони зобов'язані вжити необхідних заходів щодо користувачів і клієнтів, які використовують мережі для передачі інформації незаконного змісту. Країни, такі як Великобританія, Німеччина та Нідерланди, прийняли кодекси поведінки та створили незалежні органи, які розробляють етичні стандарти для змісту інформації та класифікації незаконної інформації [68].

З метою підвищення ефективності боротьби з кібертероризмом рекомендується реалізувати комплекс заходів:

- Розробка державної стратегії, концепції та доктрини: Розробка цих стратегічних документів в системі державного управління сталим розвитком регіону сприятиме визначенню чітких цілей та завдань у сфері кібербезпеки [69].
- Організація ефективної міжнародної співпраці: Важливо укласти угоди та розвивати співпрацю в інформаційній сфері з державами світу, їх правоохоронними органами та міжнародними організаціями. Активне співробітництво сприятиме обміну досвідом та інформацією.
- Ініціювання укладання облагороджених угод: Укладення таких угод вважається одним із найефективніших інструментів у боротьбі з кібертероризмом. Вони дозволяють об'єднати зусилля для запобігання кібератак та ефективної реакції на них.
- Створення національного відділу боротьби з кіберзлочинністю та міжнародного пункту контакту: Створення спеціалізованих структур допоможе в ефективній реалізації та запобіганні кібератак, а також сприятиме обміну

інформацією та координації дій на міжнародному рівні [69].

- Дотримання чинного законодавства та міжнародних стандартів: Застосування національного та міжнародного законодавства, зокрема Конвенції Ради Європи про боротьбу з кіберзлочинністю, є важливим елементом в протидії кіберзагрозам.

- Прийняття законів про електронну безпеку: Сучасні загрози вимагають відповідної правової бази. Прийняття законів, що регулюють електронну безпеку, сприятиме створенню ефективних механізмів захисту від кіберзлочинності та кібертероризму [69].

Згідно плану реалізації Стратегії кібербезпеки України, затвердженого рішенням Ради національної безпеки і оборони, головним пріоритетом держави є розробка системи індикаторів стану кібербезпеки. Ця система включатиме базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки, а також індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Крім того, у плані сформульовані цілі, що відображають загальну мету стратегії [69].

1. Ефективна кібероборона. Україна здійснить створення та розвиток підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі. Також буде сформована належна правова, організаційна, технологічна модель їх функціонування та застосування. Метою є забезпечення ефективної взаємодії між основними суб'єктами національної системи кібербезпеки та силами оборони під час проведення заходів з кібероборони, а також надання належного навчання та фінансового забезпечення таких структур. Планується систематичне проведення кібернавчань, оцінка спроможностей та ефективності підрозділів, а також розробка та імплементація індикаторів оцінки їхньої діяльності. Дії для досягнення цієї мети необхідно провести наступні заходи:

- Створення кібервійськ підрозділів у Міністерстві оборони України;

- Впровадження ефективних механізмів взаємодії;
- Розробка та виконання плану кібероборони;
- Проведення спільних навчань;
- Створення MIL.CERT-UA та співпраця із європейською військовою CERT-мережею [69].

2. Ефективна протидія розвідувально-підбивній діяльності у кіберпросторі та кібертероризму. Україна покладе основний акцент на забезпечення безперервного проведення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підбивної діяльності іноземних держав, актів кібершпигунства та кібертероризму. Мета полягає в усуненні умов, що сприяють цим загрозам, та причин їх виникнення для ефективного захисту інтересів держави, суспільства і окремих громадян. З цією метою необхідно реалізувати наступні заходи:

- Створення загальнодержавної системи кіберзахисту;
- Удосконалення контррозвідувального захисту кібербезпеки;
- Посилення готовності об'єктів критичної інфраструктури;
- Посилення контррозвідувального захисту сфери кібербезпеки;
- Розробка технологічних можливостей для виявлення кібератак;
- Вдосконалення боротьби з кібертероризмом [69, 70].

3. Ефективна протидія кіберзлочинності [69, 70]. Україна прагне розвинути в правоохоронних органах та державному органі спеціального призначення з правоохоронними функціями нові здібності, спрямовані на зменшення загроз кіберзлочинності та покращення їхнього технологічного та кадрового потенціалу для ефективної реалізації превентивних заходів та розслідування кіберзлочинів. З цією метою заплановані такі заходи:

- Завершити імплементацію в законодавство України положень Конвенції про кіберзлочинність;
- Забезпечити унормування в установленому порядку питання щодо

електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав - членів ЄС та враховуючи сучасні виклики і тенденції у сфері кібербезпеки;

- Розробити концептуальні підходи щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей);

- Запровадити практику проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються з кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів;

- Розробити методику збору кіберстатистики та щороку оприлюднювати статистичну інформацію щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних сайтах;

- Розробити методику проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і забезпечити проведення таких досліджень;

- Розробити методику комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створити необхідні умови для її практичної реалізації;

- Запровадити механізми ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України;

- Забезпечити в установленому порядку врегулювання правового статусу криптовалют;

- Проводити спільні з ЄС та НАТО заходи, спрямовані на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати

кіберзлочинність та реагувати на кіберзагрози;

- Забезпечити підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямками досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем та засобів;

- Забезпечити підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямками збирання та дослідження електронних доказів;

- Залучати приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів [69, 70].

4. Розвиток асиметричних інструментів стримування. Україна розвиватиме необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти країни за допомогою економічних, дипломатичних та розвідувальних заходів, а також шляхом залучення потенціалу приватного сектору. Враховуючи високий рівень загрози в цій сфері, Україна буде активно сприяти вдосконаленню кібербезпеки через ефективне взаємодію з різними секторами суспільства та міжнародними партнерами [69, 71].

5. Національна кіберготовність та надійний кіберзахист. Україна вживе конкретні та зрозумілі для всіх зацікавлених сторін заходи щодо національної кіберготовності з метою забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України. Країна збільшить рівень кіберготовності, спрямований на здатність всіх відповідальних сторін, зокрема суб'єктів сектору безпеки і оборони, ефективно та вчасно реагувати на кібератаки. Це передбачає підтримку постійної готовності до реальних та потенційних кіберзагроз, виявлення та усунення передумов для їх виникнення, забезпечення кіберстійкості, насамперед об'єктів критичної інформаційної інфраструктури.

Крім того, Україна створить національну систему управління інцидентами для координованого та ефективного вирішення кіберпроблем. Ці заходи спрямовані на зміцнення кібербезпеки країни та викликаються прагненням до найвищого рівня захисту від кіберзагроз для забезпечення стабільності і безпеки України в цифровому просторі [69, 72].

6. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки. Україна розпочне корінну реформу системи підготовки та підвищення кваліфікації фахівців у галузі кібербезпеки. Крім того, будуть прийняті заходи для збереження наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки. Ця ініціатива передбачає стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням нових кіберзагроз і викликів, а також створення національних інформаційних систем, платформ і продуктів. Національний науково-технічний потенціал буде залучатися у першу чергу для вирішення завдань забезпечення кібербезпеки держави. Особливу увагу приділятиметься розвитку цифрових навичок та кіберобізнаності, які стануть необхідними елементами освіти для кожного громадянина України. Це сприятиме створенню обізнаних та відповідальних користувачів, готових ефективно протистояти сучасним кіберзагрозам та забезпечити загальний рівень кібербезпеки в країні [69, 73].

7. Безпечні цифрові послуги. Україна забезпечить досягнення балансу між потребами суспільства, вітчизняного ринку, економіки держави та необхідними заходами з кібербезпеки, а також надійність та безпеку цифрових послуг протягом усього їхнього життєвого циклу [74].

8. Зміцнення системи координації. Україна активно буде сприяти ефективній взаємодії суб'єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки. Країна виробить умови для результативної співпраці та спільних заходів при попередженні, відбитті та нейтралізації наслідків кібератак та кіберінцидентів. Зокрема, буде забезпечено

координацію дій усіх зацікавлених сторін для подолання надзвичайних (кризових) ситуацій у кіберпросторі. Ця ініціатива передбачає встановлення ефективних механізмів співпраці та обміну інформацією між різними суб'єктами кібербезпеки, включаючи урядові організації, приватний сектор і громадські установи. Україна спрямовує свої зусилля на створення відкритого та дієвого механізму взаємодії, який дозволить ефективно реагувати на кіберзагрози та координувати спільні заходи для забезпечення кібербезпеки країни [69].

9. Формування нової моделі відносин у сфері кібербезпеки. Україна впроваджує сервісну концепцію державної участі у заходах з кіберзахисту, де держава не розглядається лише як джерело вимог, але як активний партнер у формуванні національної системи кібербезпеки. Цей інноваційний підхід передбачає встановлення партнерських відносин між урядовими структурами, приватним сектором та громадськими організаціями для спільного забезпечення ефективної захисту кіберпростору країни [69].

10. Прагматичне міжнародне співробітництво. Україна спрямовує свої стосунки з міжнародними партнерами не лише на побудову взаємної довіри для спільної відповіді на кібератаки та подолання кризових ситуацій у кібербезпеці, але й на активну практичну співпрацю. Це включає обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, а також обмін досвідом та найкращими практиками. Україна забезпечить активну участь у діалозі в рамках міжнародних організацій для спільного розроблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Координацію з міжнародними партнерами буде здійснювати Міністерство закордонних справ України [69, 75].

Зазначений вище план надає можливість задіювати велику кількість інформаційних активів для створення умов інформаційної безпеки у середовищі публічного та державного управління. Безпека інформації у стратегіях

управління в сфері публічного управління - це ключовий аспект для забезпечення ефективності та стійкості системи. Нижче наведено перероблений текст з використанням схожих ідей:

Інформаційна безпека у стратегіях публічного управління є необхідністю, що забезпечить ефективне та стійке функціонування систем управління. Основним завданням є визначення та впровадження найбільш передових підходів до захисту інформації в рамках стратегічних ініціатив публічного сектору [75].

Досягнення інформаційної безпеки передбачає використання сучасних технологій, встановлення стандартів та розробку ефективних заходів з кіберзахисту. Передусім, це включає аналіз і реагування на кіберзагрози, забезпечення конфіденційності, цілісності та доступності інформації, а також розвиток механізмів взаємодії між структурами управління для швидкого реагування на потенційні кризові ситуації.

Запровадження ефективних стратегій інформаційної безпеки в публічному управлінні включає інтеграцію передових методів, навчання персоналу, створення своєчасних механізмів виявлення та реагування на інциденти безпеки. Органи публічного управління повинні активно співпрацювати з іншими галузями та використовувати інноваційні підходи для забезпечення інтегрованого та всебічного захисту інформації.

На підставі викладеного доцільно зазначити, що первинним і основним аспектом є імплементація всіх запропонованих ідей та законодавчих вказівок безпосередньо у структуру органів управління. Насамперед, це стосується апарату органів публічного управління, таких як місцеві ради на рівні міст районів, а також офісу міських голів. Загальна стратегія забезпечення інформаційної безпеки повинна включати комплексний план дій та заходів, спрямований на забезпечення конфіденційності, цілісності та доступності інформації в рамках певної організації чи системи. Затвердження стратегії

інформаційної безпеки на рівні підприємства, установи чи організації не є виключною одиничною дією. Забезпечення інформаційної безпеки є гігантським за обсягом бізнес-процесом з політичної, технологічної та управлінської точки зору, що потребує великої кількості рішень менеджменту, інформаційно-аналітичної компетентності та обізнаності [76].

Існує безліч стандартів інформаційної безпеки, розроблених різними міжнародними та національними організаціями:

- ISO/IEC 27001: Визначає вимоги до систем управління інформаційною безпекою (СУІБ) та надає загальний підхід до управління заходами з інформаційної безпеки.
- ISO/IEC 27002: Містить конкретні рекомендації щодо застосування контрольних заходів, визначених у ISO/IEC 27001.
- NIST SP 800-53: Розроблений Національним інститутом стандартів та технологій США, надає каталог контрольних заходів для федеральних інформаційних систем та організацій.
- COBIT (Control Objectives for Information and Related Technologies): Рамковий стандарт для управління та контролю інформаційними технологіями в організації.
- PCI DSS (Payment Card Industry Data Security Standard): Визначає вимоги до захисту конфіденційної інформації про платіжні картки.

Ці стандарти визначають вимоги та рекомендації, які допомагають організаціям створювати ефективні системи управління інформаційною безпекою та забезпечувати високий рівень захисту інформації [76, 77].

Проведений аналіз теоретичних і практичних даних, що були представлені у попередніх розділах, дав нам змогу розробити та запропонувати один із варіантів типового порядку забезпечення інформаційної безпеки у структурах і апаратах органів публічного управління.

Перший етап запропонованого порядку включає затвердження стратегії

інформаційної безпеки усередині організації. Процес розробки та здійснення стратегії інформаційної безпеки організації або установи включає кілька етапів, починаючи від попередніх підготовчих робіт і закінчуючи моніторингом та оновленнями після її затвердження. Ось загальний цикл:

1. Попередній аналіз та визначення потреб:
 - Оцінка ситуації: Аналіз стану інформаційної безпеки, виявлення існуючих ризиків та вразливостей.
 - Визначення мети та обсягу: Формулювання конкретних мети та завдань стратегії.
2. Збір та аналіз вихідних даних:
 - Залучення зацікавлених сторін: Залучення ключових гравців та зацікавлених сторін для отримання різноманітних перспектив.
 - Аналіз інформації: Обробка та аналіз даних щодо існуючих систем, процесів та ризиків.
3. Розробка стратегії:
 - Визначення політик безпеки: Сформулювання основних принципів та правил для захисту інформації.
 - Визначення заходів з кіберзахисту: Встановлення конкретних заходів та технологій для запобігання та виявлення кіберзагроз.
4. Затвердження та впровадження:
 - Затвердження стратегії: Офіційне погодження стратегії інформаційної безпеки відповідними управлінськими органами.
 - Впровадження заходів: Розпочаток реалізації запланованих заходів та політик.

Цей цикл є ітеративним процесом, і організація повинна постійно вдосконалювати свою стратегію відповідно до змін в кіберзагрозах, технологічних інновацій та внутрішніх потреб.

Після затвердження Стратегії інформаційної безпеки, організація

розпочинає фазу впровадження та реалізації стратегії. Основні дії на цьому етапі включають:

- Розгортання стратегії: Формування плану розгортання стратегії, включаючи визначення відповідальних за виконання завдань та терміни їх виконання.
- Створення ділового плану: Розробка конкретного ділового плану, що включає в себе розподіл завдань, бюджетування, терміни виконання та критерії успіху.
- Розробка та впровадження політик та процедур: Створення політик та процедур інформаційної безпеки, які відповідають цілям та завданням стратегії.
- Навчання та залучення персоналу: Проведення навчань та інструктажів для персоналу з питань інформаційної безпеки, зокрема відповідно до нових політик та процедур.
- Впровадження технічних заходів: Реалізація технічних заходів, передбачених стратегією, таких як впровадження нових систем безпеки, моніторингу та захисту інформації.

Третій етап типового плану є також глобальним та не обмежений у часових рамках. Звісно після впровадження Стратегії інформаційної безпеки і виконання відповідних заходів, цикл може повторюватися, або організація може продовжувати підтримувати та актуалізувати свої заходи з інформаційної безпеки відповідно до нових викликів та технологічних змін. Це включатиме такі постійні заходи:

1. Моніторинг та аудит: Постійне відслідковування інформації з раніше встановлених систем моніторингу та проведення регулярних аудитів для визначення ефективності заходів і реагування на нові загрози.
2. Постійне вдосконалення: Впровадження процесів постійного вдосконалення системи інформаційної безпеки, враховуючи зміни в технологіях,

внутрішні та зовнішні загрози.

3. Звітність та звіти: Регулярна звітність про стан інформаційної безпеки перед керівництвом та заінтересованими сторонами.

4. Реагування на інциденти: Розроблення та впровадження плану реагування на інциденти для швидкого та ефективного реагування на події, що порушують інформаційну безпеку.

5. Актуалізація стратегії: Періодична актуалізація стратегії з урахуванням змін в загрозах, технологічних змінах та досвіду виконання попередніх заходів.

Регулярні перегляди та оновлення стратегії дозволяють організації залишатися стійкими до зростаючих загроз та забезпечувати високий рівень інформаційної безпеки в тривалій перспективі.

Висновки за розділом 3.

Визначено, що публічний сектор стикається з різноманітними загрозами та ризиками інформаційної безпеки в умовах інтенсивного використання сучасних технологій. Серед таких загроз можна виділити кібератаки, витоки даних та інші сучасні виклики.

Важливим елементом ефективного захисту є розробка та впровадження стратегій інформаційної безпеки. Сучасні ІТ-стратегії повинні враховувати комплексні заходи, спрямовані на попередження, виявлення та вирішення інформаційних загроз.

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 розділі зроблено висновки, що успішне забезпечення інформаційної

безпеки вимагає інтеграції технічних та організаційних заходів. Організації повинні не лише використовувати сучасні технології, але й встановлювати ефективні процедури та стандарти безпеки.

Важливо визначити, що інтенсивне використання інформаційних технологій вимагає постійного моніторингу і оновлення стратегій інформаційної безпеки. Загрози змінюються, тому важливо адаптувати заходи до нових викликів. На підставі інформації, що була представлена у роботі, розроблено типовий порядок забезпечення інформаційної безпеки безпосередньо у структурі органів публічного управління. Він включає 3 основні етапи від підготовки та розробки стратегії інформаційної безпеки до впровадження політик, технічних засобів а також безперебійну підтримку і моніторинг.

Цей розділ визначає ключові вектори дій для забезпечення ефективної інформаційної безпеки в умовах інтенсивного використання сучасних інформаційних технологій у публічному секторі та наголошує на важливості комплексного підходу.

ВИСНОВКИ

Підбиваючи підсумок, можна констатувати, що в сучасному світі революція інформаційних технологій перепрограмує всі сфери громадського життя, включаючи публічне управління. Зростаюча комп'ютеризація та автоматизація процесів, пов'язаних з державним управлінням, накладають великі виклики та вимагають глибокого розуміння впливу інформаційних технологій на ефективність та безпеку адміністративних процедур.

Аналіз потенціалу інформаційних технологій показав, що вони можуть стати ефективним інструментом для оптимізації процесів публічного адміністрування. Впровадження систем електронного урядування дозволяє автоматизувати багато аспектів роботи державних установ, забезпечуючи швидкий та ефективний доступ до послуг для громадян.

Інформаційні технології стали ключовим фактором у вдосконаленні урядової діяльності та наданні послуг громадянам, відкриваючи нові можливості для підвищення ефективності та транспарентності публічного адміністрування. Інновації в свою чергу є невід'ємним елементом сучасного суспільства, визначаючи його подальший розвиток та успішність. Поняття інновацій охоплює впровадження новаторських ідей, технологій, продуктів та методів у різних сферах життя.

Сучасні інноваційні рішення, такі як смарт-міста та технології Інтернету речей, сприяють оптимізації управління енергоспоживанням та транспортом. Електронне здоров'я та електронне освітнє середовище полегшують доступ до медичних та освітніх послуг. Фінансові технології, соціальні мережі та електронна демократія відкривають нові шляхи для підвищення ефективності та участі громадян у процесах управління, зміцнюючи конкурентоспроможність суспільства.

Інформаційні та комунікаційні технології в публічному управлінні є

корисними, оскільки забезпечують:

- Широкий доступ до інформації.
- Ефективне використання часу та ресурсів.
- Відкритий доступ до публічних послуг.
- Забезпечення безпеки даних.

Ці фактори забезпечуються інноваційним управлінням, що представляє собою систему керування, спрямовану на створення умов для розвитку та ефективного впровадження інновацій в організації.

В роботі зазначені новітні тенденції та технологічні інновації в галузі публічного управління включають елементи:

- Електронного урядування (e-Government).
- Заходи кібербезпеки.
- Дистанційної освіти
- Електронні системи управління проектами тощо.

В цьому контексті були запропоновані на огляд, низка реалізованих українських та зарубіжних продуктів, які відображають всі тенденції використання технологічних інновацій в галузі управління як на державному рівні так і на місцевому. Таким чином зафіксовано що впровадження новітніх технологій в публічному управлінні націлене на поліпшення якості життя громадян та забезпечення ефективності урядової діяльності.

У другому розділі роботи приділено увагу системам електронного урядування як основного елемента інформаційних технологій у сфері публічного адміністрування. Висвітлені історичні аспекти розвитку електронного урядування, що включає в себе 2 етапи.

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

- Централізована модель.
- Децентралізована модель.

Крім того існує низка індексів та прикладів стратегій, а також додаткових практичних моделей для оцінки прогресу електронного урядування. Кожне з запропонованих моделей та індексів включає різні етапи. Важливою є ідея того, що перехід від одного етапу до іншого відбувається етапно, і кожен наступний етап включає покращення та розширення функціоналу.

Також представлена таблиця спільних викликів та бар'єрів на основі літературного огляду, що можуть затримати розвиток електронного урядування при його впровадженні. Цей фактор надає нам можливість зробити висновок, що впровадження електронного уряду не є простим завданням і стикається з численними проблемами та бар'єрами, які вимагають уважного вивчення та вирішення.

В ході вивчення законодавства виявлено, що в контексті публічного і державного адміністрування система працює для забезпечення наступних цілей:

- Створення єдиної бази даних для державних службовців та працівників органів впровадження.
- Автоматизація та цифровізація управління людськими ресурсами та кадрових рішень.
- Моніторинг результативності діяльності в органах впровадження у сфері управління персоналом.
- Забезпечення прозорості та доступності інформації про людські ресурси та оплату праці.
- Посилення спроможності структурних підрозділів управління персоналом та бухгалтерського обліку.
- Розвиток сучасного управління людськими ресурсами через оперативність та надійність обліку.
- Функціонування інформаційної системи на державній службі та електронна взаємодія.
- Електронна взаємодія між органами впровадження та надання

доступу до інформації працівникам.

Вказані цілі і є основними напрямками, що вказують на роль інформаційних систем управління в оптимізації процесів публічного адміністрування.

Загалом зазначено, що інформаційні технології визначають потенціал для трансформації управлінських підходів у публічному адмініструванні, підкреслюючи їх важливість у досягненні високої ефективності та підтримки взаємодії між урядом та громадянами.

Потреба в ефективному захисті інформації обумовлена не лише внутрішніми потребами держави, але й зобов'язаннями перед громадянами. Збереження конфіденційної інформації є важливою місією державних структур, оскільки їхній недолік може призвести до технічних проблем і порушення довіри громадськості, що негативно впливає на легітимність та дієздатність владних органів.

За результатами вивчених даних з різних джерел, виділено основні загрози для інформаційної безпеки в публічному секторі:

- Кібератаки, та кіберзлочинність в загальному розумінні;
- Витік конфіденційної інформації.

Також в роботі висвітлені основні виклики пов'язані з інформаційною безпекою, які стали реаліями війни. Для загального розуміння наданий приблизний перелік, каналів витоку інформації, який включає як прямі так і опосередковані дії.

Наслідками для урядових органів та громадськості в разі витоку конфіденційної інформації може стати: втрата довіри до урядових структур, підвищений ризик корупції, загрозу національній безпеці, особливо в сфері оборони, та можливу втрату конкурентної переваги урядових органів у сфері економіки.

У заключному підрозділі було проведено аналіз, великої кількості,

міжнародних стандартів з інформаційної безпеки. На підставі зібраної інформації та аналізу джерел представлених у роботі було запропоновано варіантів типового порядку забезпечення інформаційної безпеки у структурах і апаратах органів публічного управління. Він включає наступні етапи:

- Попередній аналіз та визначення потреб включає оцінку ситуації, визначення мети та обсягу, збір та аналіз вихідних даних, залучення зацікавлених сторін та аналіз інформації.
- Розробка стратегії охоплює визначення політик безпеки та заходів з кіберзахисту.
- Затвердження та впровадження включає затвердження стратегії та впровадження заходів.
- Розгортання стратегії, створення ділового плану, розробка та впровадження політик та процедур, навчання та залучення персоналу, і впровадження технічних заходів є ключовими етапами в цьому процесі.

Після впровадження Стратегії інформаційної безпеки і виконання заходів, цикл може повторюватися, або організація може продовжувати підтримувати та актуалізувати свої заходи з інформаційної безпеки відповідно до нових викликів та технологічних змін. Це включатиме такі постійні заходи:

- Моніторинг та аудит, включаючи системи моніторингу та аудитів, для оцінки ефективності заходів і реагування на загрози.
- Постійне вдосконалення системи інформаційної безпеки, враховуючи технологічні та загрози.
- Регулярна звітність про стан інформаційної безпеки перед керівництвом і сторонами.
- Реагування на інциденти через розробку та впровадження плану.
- Періодична актуалізація стратегії з урахуванням змін в загрозах та технологіях.

Узагальнюючи проведене дослідження можна зазначити, що інформаційні

технології в публічному адмініструванні значно полегшують роботу урядових органів, прискорюють надання послуг та забезпечують ефективний обмін інформацією. Однак їх використання також створює нові виклики для інформаційної безпеки, вимагаючи постійного вдосконалення стратегій та заходів для захисту конфіденційної інформації від різноманітних загроз. Співвідношення між вигодами ІТ та потребами в ефективному кіберзахисті стає важливим аспектом сучасного управління державними справами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Manning N., Blum J., Srivastava V. Public Sector Management Reform : Toward a Problem-Solving Approach. Handle Proxy. URL: <http://hdl.handle.net/10986/17057> (дата звернення: 20.11.2023).
2. Dahlgren P. The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation. Political Communication. 2005. Т. 22, № 2. С. 147–162. URL: <https://doi.org/10.1080/10584600590933160> (дата звернення: 17.11.2023).
3. Bünte M. The authoritarian public sphere. Legitimation and autocratic power in North Korea, Burma, and China. Democratization. 2019. Т. 27, № 1. С. 159–160. URL: <https://doi.org/10.1080/13510347.2019.1619701> (дата звернення: 16.11.2023).
4. The Innovation Imperative in the Public Sector: Setting an agenda for action - Observatory of Public Sector Innovation. Observatory of Public Sector Innovation. URL: <https://oecd-opsi.org/publications/the-innovation-imperative/> (дата звернення: 01.11.2023).
5. Dhingra D., Dabas A. Global Strategy on Digital Health. Indian Pediatrics. 2020. Т. 57, № 4. С. 356–358. URL: <https://doi.org/10.1007/s13312-020-1789-7> (дата звернення: 20.11.2023).
6. Commission E. Missing Entrepreneurs 2021 Policies for Inclusive Entrepreneurship and Self-Employment. Organization for Economic Cooperation & Development, 2021.
7. Digital Government in the Decade of Action for Sustainable Development. New York : Department of Economic and Social Affairs, 2015. 323 с. URL: [https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20\(Full%20Report\).pdf](https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf) (дата звернення: 02.06.2023).
8. Global strategy on digital health 2020-2025. Geneva, 2020. 57 p. URL:

<https://iris.who.int/bitstream/handle/10665/344249/9789240020924-eng.pdf?sequence=1&isAllowed=y> (дата звернення: 28.07.2023).

9. Smart Cities Solutions for More Flood Resilient Communities / К. Carlson та ін. 2019 Systems and Information Engineering Design Symposium (SIEDS), м. Charlottesville, VA, USA, 26 квіт. 2019 р. 2019. URL: <https://doi.org/10.1109/sieds.2019.8735625> (дата звернення: 20.11.2023).

10. Герасимюк Л.С., Тарасюк Л.М. Використання сучасних ІКТ у публічному управлінні: проблеми та перспективи. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. 2021. Т. 32, № 4. С. 34–39.

11. Chavez N., Kounang N. A man diagnosed with Wuhan coronavirus near Seattle is being treated largely by a robot | CNN. CNN. URL: <https://www.cnn.com/2020/01/23/health/us-wuhan-coronavirus-doctor-interview/index.html> (дата звернення: 20.09.2023).

12. Loh T., Fishbane L. COVID-19 makes the benefits of telework obvious.. Available at. 2020. URL: <https://www.brookings.edu/blog/the-avenue/2020/03/17/covid-19-makes-the-benefits-of-telework-obvious> (дата звернення: 10.05.2023).

13. Ben-Assuli O., Padman R. Trajectories of repeated readmissions of chronic disease patients: Risk stratification, profiling, and prediction. MIS Quarterly. 2020;44(1):201–226.

14. Making Education a Priority in the Post-2015 Development Agenda - NEW REPORT!. UNESCO : Building Peace through Education, Science and Culture, communication and information. URL: <https://www.unesco.org/en/articles/making-education-priority-post-2015-development-agenda-new-report> (дата звернення: 24.08.2023).

15. How to develop soft skills. McKinsey & Company. URL: <https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-organization-blog/how-to-develop-soft-skills> (дата звернення: 24.08.2023).

05.07.2023).

16. Pliushch V., Sorokun S. Innovative Pedagogical Technologies in Education System. *Revista Tempos e Espaços em Educação*. 2022. Т. 15, № 34. С. e16960. URL: <https://doi.org/10.20952/revtee.v15i34.16960> (дата звернення: 6.10.2023).

17. Froomkin A. M. M. Habermas@discourse.net: Toward a Critical Theory of Cyberspace. *SSRN Electronic Journal*. 2003. URL: <https://doi.org/10.2139/ssrn.363840> (дата звернення: 05.07.2023).

18. Bohman J. Expanding Dialogue: The Internet, the Public Sphere and Prospects for Transnational Democracy. *The Sociological Review*. 2004. Т. 52, № 1_suppl. С. 131–155. URL: <https://doi.org/10.1111/j.1467-954x.2004.00477.x> (дата звернення: 06.07.2023).

19. Громадянське суспільство в Україні: становлення та розвиток : навч. посіб. / кол. авт. : А. М. Михненко, С. О. Кравченко, І. В. Пантелейчук та ін. – К. : УкрСІЧ, 2015. – 347 с.

20. Енциклопедія державного управління : у 8 т. / наук.-ред. колегія : Ю.В. Ковбасюк (голова) та ін. – К. : НАДУ, 2011. – Т. 1 : Теорія державного управління. – 2011. – 748 с.

21. Аль-Атті І., Коцур В. Теоретичні підходи до проблеми розвитку сучасної моделі публічного управління. *Наукові перспективи (Naukovі perspektivi)*. 2021. № 5 (11). URL: [https://doi.org/10.52058/2708-7530-2021-5\(11\)-26-33](https://doi.org/10.52058/2708-7530-2021-5(11)-26-33) (дата звернення: 07.07.2023).

22. Makarenko M. Public administration in the conditions of an extraordinary epidemiological situation: essence and basic categories. *Electronic scientific publication "public administration and national security"*. 2023. № 3(33). URL: <https://doi.org/10.25313/2617-572x-2023-3-8806> (дата звернення: 20.07.2023).

23. Сидоренко Н. Сучасні тенденції розвитку публічного управління. *Public administration aspects*. 2022. Т. 10, № 3. С. 59–63. URL:

<https://doi.org/10.15421/152220> (дата звернення: 20.07.2023).

24. Про місцеве самоврядування в Україні : Закон України від 21.05.1997 р. № 280/97-ВР : станом на 3 серп. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/280/97-вр#Text> (дата звернення: 20.07.2023).

25. Битяк Ю. Адміністративне судочинство як форма забезпечення верховенства права і законності. Право України. 2011. № 4. С. 4–11.

26. Гончарук Н. Т. Вплив розвитку громадянського суспільства на публічне управління / Н. Т. Гончарук, І. Г. Сурай // Галузь науки «Державне управління» історія, теорія, впровадження: матеріали наук.-практ. конф. за міжнар. участю, Київ, 28 трав. 2010 р. : у 2 т. – Київ: НАДУ, 2010. – Т. 1. – С. 145-146.

27. Про місцеве самоврядування в Україні : Закон України від 21.05.1997 р. № 280/97-ВР : станом на 3 серп. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/280/97-вр#Text> (дата звернення: 11.11.2023).

28. Савченко С., Шенгер М. Принципи стратегічного управління ефективністю діяльності підприємства. Grail of science. 2022. № 17. С. 66–68. URL: <https://doi.org/10.36074/grail-of-science.22.07.2022.008> (дата звернення: 21.11.2023).

29. Миронова О. В. Інновації і підприємництво як чинник підвищення конкурентоспроможності вітчизняних підприємств : thesis. 2017. URL: <https://er.knutd.edu.ua/handle/123456789/10212> (дата звернення: 04.09.2023).

30. Шкуропат О. Досвід країн Європейського Союзу в державному управлінні земельними відносинами. Державне управління та місцеве самоврядування. 2013. Вип. 3 (18). С. 186–197.

31. Колісник Г. М. Критичний аналіз сучасного стану системи управління витратами в контексті державного регулювання. Актуальні проблеми економіки. 2016. № 8 (182). С. 62–68.

32. Про внесення змін до Положення про Єдиний державний веб-портал

цифрової освіти “Дія. Цифрова освіта” : Постанова Каб. Міністрів України від 16.09.2022 р. № 1032. URL: <https://zakon.rada.gov.ua/laws/show/1032-2022-п#Text> (дата звернення: 20.08.2023).

33. Про нас | ProZorro. Головна | Prozorro. URL: <https://prozorro.gov.ua/about> (дата звернення: 06.09.2023).

34. Digital Dubai Authority. URL: <https://www.digitaldubai.ae/> (дата звернення: 07.09.2023).

35. From dream to reality: Developing sustainable smart cities in the United Arab Emirates - ITU Hub. ITU Hub. URL: <https://www.itu.int/hub/2020/08/from-dream-to-reality-developing-sustainable-smart-cities-in-the-united-arab-emirates/> (дата звернення: 07.09.2023).

36. E-Estonia Programme for e-Government - e-Estonia. e-Estonia. URL: <https://e-estonia.com/programme/e-government/> (дата звернення: 07.09.2023).

37. Державні послуги онлайн. Державні послуги онлайн. URL: <https://plan2.diia.gov.ua/projects> (дата звернення: 08.09.2023).

38. Відбулася сесія Одеської міської ради. Офіційний сайт міста Одеси. URL: <https://omr.gov.ua/ua/news/222667/> (дата звернення: 05.07.2023).

39. United Nations e-government survey 2008: from e-government to connected governance / ред. United Nations. Division for Public Administration and Development Management. New York : United Nations, 2008. 224 с.

40. Kassahun A. E., Molla A., Sarkar P. Government process reengineering. Digital democracy. 2012. С. 1730–1752. URL: <https://doi.org/10.4018/978-1-4666-1740-7.ch086> (дата звернення: 21.11.2023).

41. Grafton C. Book review: implementing and managing e-government: an international text. Social science computer review. 2006. Т. 24, № 3. С. 389–391. URL: <https://doi.org/10.1177/0894439306287246> (дата звернення: 21.11.2023).

42. Fountain J. E. Building the virtual state: information technology and institutional change. Brookings Institution Press, 2001. 256 с.

43. 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).

44. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядж. Каб. Міністрів України від 20.09.2017 р. № 649-р. URL: <https://zakon.rada.gov.ua/laws/show/649-2017-p#Text> (дата звернення: 21.09.2023).

45. Залучення громадян до розробки та ухвалення рішень місцевим самоврядуванням. Київ : ЗЕЛ. КН.: ЦЕНТР UA, 2018. 82 с. URL: <https://centreua.org/wp-content/uploads/2021/07/Zaluchennya-gromadyan-do-rozrobky-ta-uhvalennya-rishen-mistsevym-samovryaduvannya.pdf> (дата звернення: 13.09.2023).

46. Маркевич К. Цифровізація: переваги та шляхи подолання викликів. Центр Разумкова. URL: <https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv> (дата звернення: 13.09.2023).

47. What is digital government?. Gartner. URL: <https://www.gartner.com/en/topics/digital-government> (дата звернення: 14.09.2023).

48. Garcia-Garcia L. M., Gil-Garcia J. R., Gómez V. Citizen centered e-government?. Dg.o 2015: 16th annual international digital government research conference, Phoenix Arizona. New York, NY, USA, 2015. URL: <https://doi.org/10.1145/2757401.2757457> (дата звернення: 15.09.2023).

49. Nikkhahan B., Tarokh M. J. Citizen lifetime value in e-government. Managing customer trust, satisfaction, and loyalty through information communication technologies. 2013. С. 202–218. URL: <https://doi.org/10.4018/978-1-4666-3631-6.ch012> (дата звернення: 20.19.2023).\

50. Гавриленко Т. Упровадження сучасних технологій в органах місцевого самоврядування України на прикладі міста Києва. Юридичний науковий електронний журнал. 2021. С. 18–20. URL: http://www.lsej.org.ua/9_2021/4.pdf (дата звернення: 07.09.2023).

51. Шевченко А. В. Управління функціональною стійкістю інформаційних систем на основі оптимізації видатків на захист. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняхівського. 2019. № 3-64. С. 90–96. URL: <https://doi.org/10.33099/2304-2745/2018-3-64/90-96> (дата звернення: 27.11.2023).

52. Юдкова К. В. Особливості визначення поняття "інформаційна система". Інформація і право. 2015. № 2 (14). С. 39–44.

53. Шаповал В. М. Конституційне право зарубіжних країн : Підруч. для студ. юрид. вищ. навч. закл. і фак-тів. Київ : АртЕк, Вища шк., 1997. 264 с.

54. Міхровська М. Адміністративна реформа та цифрове урядування: нова точка відліку. Modalități conceptuale de dezvoltare a științei moderne. 2020. URL: <https://doi.org/10.36074/20.11.2020.v4.08> (дата звернення: 23.09.2023).

55. Про затвердження Положення про інформаційну систему управління людськими ресурсами в державних органах : Постанова Каб. Міністрів України від 28.12.2020 р. № 1343 : станом на 28 верес. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/1343-2020-п#Text> (дата звернення: 17.08.2023).

56. Про Національну програму інформатизації : Закон України від 04.02.1998 р. № 74/98-ВР : станом на 1 берез. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/74/98-вр#Text> (дата звернення: 17.08.2023).2

57. Про Стратегію інформаційної безпеки : Рішення Ради нац. безпеки і оборони України від 15.10.2021 р. : станом на 30 груд. 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/n0080525-21#Text> (дата звернення: 17.08.2023).

58. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. ОПЕР. ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЕРЖ. ЦЕНТРУ КІБЕРЗАХ. ДЕРЖ. СЛУЖБИ СПЕЦ. ЗВ'ЯЗКУ ТА ЗАХ. ІНФОРМАЦІЇ УКРАЇНИ, 2023. URL: <https://scpc.gov.ua/api/files/a7de388d-14d3-4248-b8be->

ada8b5cb0710 (дата звернення: 11.08.2023).

59. Швайка Д. О. Функції комунікативного менеджменту в захисті інформації. Інформація як об'єкт захисту : thesis. 2016. URL: <http://dspace.kntu.kr.ua/jspui/handle/123456789/4174> (дата звернення: 11.10.2023).

60. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. Сучасний захист інформації. 2015. № 4. С. 86–90.

61. Думчиков М. О., Думчиков М. А., Dumchykov M. O. Кібератаки як новітня загроза інформаційній безпеці : thesis. 2020. URL: <https://essuir.sumdu.edu.ua/handle/123456789/77915> (дата звернення: 12.10.2023).

62. Твердохліб Ю. М. Інформаційно-психологічні операції у російсько-українській гібридній війні : автореф. дис. ... канд. політ. наук. Чернівці, 2020. 16 с.

63. An overview of Russia's cyberattack activity in Ukraine. Digital Security Unit, 2022. URL: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd> (дата звернення: 19.10.2023).

64. Делембовський М., Терентьев О., Корнійчук Б. Людський фактор у розголошенні конфіденційної та приватної інформації. Grail of science. 2023. № 24. С. 347–350. URL: <https://doi.org/10.36074/grail-of-science.17.02.2023.063> (дата звернення: 19.10.2023).

65. Чеботарьова Д. В., Пестерева С. Є. Аналіз технологій запобігання витоку інформації : thesis. 2021. URL: <https://openarchive.nure.ua/handle/document/18670> (дата звернення: 19.10.2023).

66. Горліченко С. Особливості формування технічних каналів витоку інформації від сучасних ікс. Ukrainian scientific journal of information security. 2023. Т. 29, № 2. С. 80–87. URL: <https://doi.org/10.18372/2225-5036.29.17872> (дата звернення: 19.10.2023).

67. Nikkhahan B., Tarokh M. J. Citizen lifetime value in e-government. Managing customer trust, satisfaction, and loyalty through information communication technologies. 2013. С. 202–218. URL: <https://doi.org/10.4018/978-1-4666-3631-6.ch012> (дата звернення: 12.11.2023).

68. Колос О., Каленська К. Еволюція розділу хві 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).

69. Про План реалізації Стратегії кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 30.12.2021 р. : станом на 3 лют. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text> (дата звернення: 11.10.2023).

70. Самойленко О. Протидія кримінальним правопорушенням, учиненим у кіберпросторі, як новий напрям криміналістики. Право України. 2021. № 2021/08. С. 131. URL: <https://doi.org/10.33498/loou-2021-08-131> (дата звернення: 27.10.2023).

71. Смородська Д. Р. Мова національної єдності у протистоянні російській агресії. Соціальні комунікації: інструменти, технологія і практика. 2023. URL: <https://doi.org/10.36059/978-966-397-313-5-20> (дата звернення: 27.10.2023).

72. Лук"яненко Л. Г. Національна ідея і національна воля. Київ, 2006. 288 с.

73. Хаханова Г., Абдуллаєв В. Відношення між відношеннями кібер-соціального комп'ютингу. Modern engineering and innovative technologies. 2019. № 23-01. С. 44–60. URL: <https://doi.org/10.30890/2567-5273.2022-23-01-022> (дата звернення: 27.10.2023).

74. Сай В. І. Вплив закону про цифрові послуги (the digital service act) на

діяльність онлайн-медіа в Україні. Juridical scientific and electronic journal. 2023. № 8. С. 159–161. URL: <https://doi.org/10.32782/2524-0374/2023-8/35> (дата звернення: 28.10.2023).

75. Тормахова А. Міжнародне співробітництво в організації сучасних українських проєктів. Українська культура : минуле, сучасне, шляхи розвитку (напрямок: культурологія). 2022. № 43. С. 77–81. URL: <https://doi.org/10.35619/ucpmk.vi43.584> (дата звернення: 27.10.2023).

76. Кравченко Д. А. Міжнародно-правові стандарти у сфері забезпечення міжнародної інформаційної безпеки : магістерська робота. 2020. URL: <https://dspace.znu.edu.ua/jspui/handle/12345/3535> (дата звернення: 20.11.2023).

77. Information security controls. Iso/iec 27001:2022. 2022. Р. 28–36. URL: <https://doi.org/10.2307/j.ctv30qq13d.8> (дата звернення: 27.10.2023).