ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ
Кафедра публічного управління та адміністрування

МАГІСТЕРСЬКА РОБОТА

на тему:

«НАПРЯМИ ТРАНФОРМАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ЦИФРОВОГО СУСПІЛЬСТВА»

Виконала: студентка магістратури за спеціальністю
281 Публічне управління та адміністрування
Дар'я ЯКИМЧУК

Керівник: кандидатка наук з державного управління, доцентка**,**
Людмила ТРЕБИК

Рецензент: _____

(науковий ступінь, вчене звання, прізвище та ініціали)

Хмельницький – 2022 рік

АНОТАЦІЯ

Якимчук Даря Леонідівна. Напрями трансформації сфери публічного управління в умовах цифрового суспільства. – Рукопис.

Стрімке впровадження цифрових технологій в усі аспекти життя громадськості провокує необхідність трансформації діяльності публічного управління в умовах цифрового суспільства.

Цифрове суспільство є молодим та перспективним напрямом дослідження у сучасній науці. Шляхи трансформації діяльності органів публічного управління є засобом створення комунікаційних містків між державною та суспільством, запорукою підсилення демократичності держави, що відображається у відкритості та прозорості її діяльності.

У досліджені відображуються різні аспекти впровадження цифрових технологій у роботі держаних службовців. За основу взято роботу Антимонопольного комітету України у особі Південно-західного міжобласного територіального Відділення.

Розглянуто питання взаємодії сфер публічного управління, цифрового суспільства, цифровізації, діджиталізації, цифрової держави, кіберпростору, кібербезпеки, нормативно-правове регулювання досліджуваної теми, принципи дії, а, також, висвітлені основні шляхи реалізації трансформації органів публічного управління в умовах цифрового суспільства.

Створено опитування у онлайн-ресурсі Google Forms для працівників Південно-західного міжобласного територіального відділення Антимонопольного комітету України щодо оцінки цифрової компетентності державного службовця до вимог цифрового суспільства. Відповідно до аналізу анкет зроблено висновки щодо сучасного рівня цифрової компетенції державних службовців.

Ключові слова: публічне управління, цифрове суспільство, цифровізація, цифрова держава, цифрова трансформація, діджиталізація, кіберпростір, кібернебезпека, кіберзахист.

ANNOTATION

Daria Leonidivna Yakymchuk. Directions of transformation of the sphere of public administration in the conditions of a digital society. - Manuscript.

The rapid introduction of digital technologies into all aspects of public life provokes the need to transform public administration activities in the conditions of a digital society.

Digital society is a young and promising field of research in modern science. Ways of transforming the activities of public administration bodies are a means of creating communication bridges between the state and society, a key to strengthening the democracy of the state, which is reflected in the openness and transparency of its activities.

Various aspects of the implementation of digital technologies in the work of civil servants are reflected in the study. The basis is the work of the Antimonopoly Committee of Ukraine represented by the South-Western Interregional Territorial Branch.

The issue of the interaction of the spheres of public administration, digital society, digitization, digitization, digital state, cyberspace, cyber security, regulatory and legal regulation of the researched topic, principles of action, and the main ways of implementing the transformation of public administration bodies in the conditions of a digital society are considered.

A survey was created in the Google Forms online resource for employees of the South-Western Interregional Territorial Branch of the Antimonopoly Committee of Ukraine regarding the assessment of the digital competence of a civil servant to the requirements of a digital society. According to the analysis of the questionnaires, conclusions were made regarding the current level of digital competence of civil servants.

Keywords: public administration, digital society, digitalization, digital state, digital transformation, digitalization, cyberspace, cyber security, cyber protection.

ЗМІСТ

ВСТУП

Актуальність теми. Відповідно до Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації важливим є дослідження напрямів трансформації сфери публічного управління в умовах цифрового суспільства. Впровадження цифрових технологій є надзвичайно стрімким та тривалим процесом, що несе у собі масу нових викликів як для суспільства, так і для держави. Динамічність даного процесу провокує створення та розвиток нового цифрового суспільства, а також цифровізації держави в цілому.

При необхідності швидкої та якісної трансформації органів державної влади до умов цифрового суспільства виникає потреба у якісному регулюванні впровадження та використання цифрових технологій на законодавчому рівні.

Концепцію електронної держави варто розглядати як проект, що спрямований на реалізацію демократії, розвитку форм комунікації громадян із державою через органи державної влади та органи місцевого самоврядування.

Створення дієвих механізмів оцифровування органів державної влади та засобів пристосування державного управління до умов цифрового суспільства є пріоритетом на шляху до створення максимально демократичної держави. Варто зазначити що дана тема є досить молодою та мало вивченою через швидкість впровадження цифровізації в Україні.

У науковій роботі відображуються різні аспекти впровадження цифрових технологій у роботі держаних службовців. За основу взято роботу Антимонопольного комітету України у особі Південно-західного міжобласного територіального Відділення.

Рівень висвітлення досліджуваної теми в науковій літературі. Питання цифрової держави розглядалися такими науковцями як: Бойко Н.,

Мохова Ю.Л., Духовна О., Бурдін М. Ю., Поченчук Г., Данилов А. Д., Соловйова К. О., Турченко Ю. В., Збожинський С., Матвієнко О., Мурач Д., Теліженко Л., Татарінцева А. В., Степанов В. Ю., Оболенський О. та інші.

Мета та завдання. Мета магістерської роботи полягає у досліджені теоретичних засад цифрового суспільства та його вплив на публічне управління, аналізу шляхів трансформації діяльності антимонопольного комітету в умовах розвитку цифрового суспільства та висвітленні питання кібербезпеки як основи взаємодії органів публічного управління з громадян у аспекті захисту інформації.

Для досягнення поставленої мети вирішуються наступні завдання:

1) дослідити поняття публічного управління, цифрового суспільства, цифрової держави, цифровізації, діджиталізації, електронного врядування, їх ознаки та принципи;

2) висвітлити нормативно-правове регулювання цифровізації у сфері публічного управління.

3) дослідити інструменти трансформації органів публічних органів в умовах цифрового суспільства на прикладі Антимонопольного комітету України.

4) оцінити зміни стратегії трансформації публічного управління в умовах цифрового суспільства.

5) оцінити рівень трансформації органів публічного управління в умовах цифрового суспільства на прикладі Антимонопольного комітету України.

6) дослідження кібербезпеки як основи взаємодії органів публічного управління з громадян у аспекті захисту інформації.

Предмет дослідження. Шляхи трансформації публічного управління в умовах цифрового суспільства.

Об’єкт дослідження. Суспільні відносини органів публічного управління в умовах цифрового суспільства.

Методи дослідження. На кожному етапі дослідження, відповідно до поставлених запитань використовувалися як зальні, та і спеціальні методи. Метод аналізу використовувався при опрацюванні законодавчого регулювання питання трансформації та аналізу опитування державних службовців. Метод узагальнення було використано для виявлення рівня цифрової трансформації органів публічного управління.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЦИФРОВОГО СУСПІЛЬСТВА ТА ЙОГО ВПЛИВ НА ПУБЛІЧНЕ УПРАВЛІННЯ

1.1 Поняття публічного управління, цифрового суспільства, їх ознаки та принципи

Термін «публічне управління» (з англ. public management) вперше застосував англійський державний службовець Десмонд Кілінг у 1972 р., який трактував його наступним чином: публічне управління – це пошук у найкращий спосіб використання ресурсів задля досягнення пріоритетних цілей державної політики.

Публічне управління – це організуючий і регулюючий вплив держави на суспільну життєдіяльність людей з метою її впорядкування, збереження чи перетворення, опираючись на владну силу, яку обмежує дієвий суспільний контроль [14].

Органи публічного управління є певним містком між державою та суспільством. Саме тому взаємодія них органів з суспільством є першочерговим аспектом роботи.

Публічне управління характеризується такими ознаками:

1) Ієрархічність, що відображається в організації діяльності органів публічного управління у вигляді впровадження субординації та чіткої підпорядкованості.

2) Підзаконність, яка є основою регулювання діяльності публічного управління за допомогою норм чинного законодавства.

3) Суспільна орієнтованість є проявом першочергового вияву ідеї функціонування публічного управління, що характеризується службою народу України.

4) Виконавчо-розпорядчий характер відображає контроль за виконанням виконавчих приписів шляхом здійснення розпорядчих дій.

5) Маштабність означає об’єми реалізації управлінської діяльності, включаючи сфери управлінського впливу: політична, соціальна, екологічна,

економічна, фінансова, інформаційна, тощо. Дії органів публічного управління поширюються на усю територію України.

6) Універсальність виражається можливості отримання необхідних послуг в незалежності до місця перебування, безперервності виконання повноважень охоплюючи усі сфери управлінського впливу.

Цифрове суспільство — це суспільство, яке інтенсивно та продуктивно використовує цифрові технології для власних потреб (самореалізація, робота, відпочинок, навчання, дозвілля кожного), а також для досягнення та реалізації спільних економічних, суспільних та громадських цілей [15].

Цифрова трансформація ґрунтується на змінах діяльності із переходом до використання інформаційних та цифрових технологій в усіх робочих процес.

Цифровізація з точки зору публічного управління це перенесення усіх аспектів діяльності у смартфон.

Поняття «цифрової держави» є більш абстрактним. Воно описує сворення держави, яка є мобільною, містить можливість об’єднання різних відомств, структур та інших органів державної влади у одну величезну онлайн-систему, що, в першу чергу, буде дієво виконувати свої функції, стане більш відкритою та прозорою, зрозумілою та зручною для будь-якого користувача.

Цифровізацію варто розглядати як інструмент, а не як самостійну ціль. За системного державного підходу цифрові технології стимулюватимуть створення робочих місць, підвищення продуктивності, темпів економічного зростання та якості життя громадян України.

Так, у Концепції розвитку цифрової економіки та суспільства України сформульовано основні принципи цифровізації (таб. 1.1) , що є визначальними для створення й реалізації переваг впровадження цифрових технологій та користування ними.

Принцип 1. Цифровізація повинна забезпечувати кожному громадянинові рівний доступ до послуг, інформації та знань, що надаються на основі інформаційно-комунікаційних та цифрових технологій.	**Принцип 2.** Цифровізація повинна бути спрямована на створення переваг у різних сферах повсякденного життя.
Принцип 3. Цифровізація є інструментом економчного зростання шляхом підвищення ефективності, продуктивності та конкурентоздатно-сті завдяки використанню цифрових технологій.	**Принцип 4.** Цифровізація повинна сприяти розвитку інформаційного суспільства та засобів масової інформації шляхом створення якісного контенту, насамперед українського.
Принцип 5. Цифровізація повинна орієнтуватися на міжнародне, європейське та регіональне співробітництво з метою інтеграції України до ЄС, виходу на європейський і світовий ринок.	**Принцип 6.** Стандартизація є основою цифровізації, одним із головних чинників її успішної реалізації. Побудова лише на українських стандартах цифрових систем, платформ та інфраструктур, які мають бути використані громадянами, бізнесом та державою.
Принцип 7. Цифровізація повинна супроводжуватися підвищенням рівня довіри й безпеки. Інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій.	**Принцип 8.** Цифровізація як об'єкт фокусного та комплек-сного державного управління. Починаючи із становлення України як самостійної та незалежної держави залишається таке поняття як «бюрократизм» який залишив слід у роботі державних органів.

Таб. 1.1 – Основні принципи цифровізації

Електронне врядування - спосіб організації місцевого самоврядування за допомогою програмно-апаратних засобів та систем локальних інформаційних мереж, що забезпечує відкритість та прозорість функціонування органу місцевого самоврядування, завчасний та повний

доступ до інформації щодо діяльності органу, просте і доступне щоденне спілкування з місцевою владою громадян, представників бізнесу та неурядових організацій.

Практичність використання електронного врядування, що є одним із найбільш практичних на сьогодні відображань цифрового суспільства у публічному управлінні, нівелює високий рівень бюрократії, чим покращує комунікаційні містки держави та суспільства у цілому, а, також, знижує рівень конфліктних ситуацій.

Неабиякий позитивний аспект впровадження електронного врядування є вирішення різного виду питань без фізичної присутності особи без крайньої необхідності. Економія часу та відсутність «біготні» є величезною перевагою цифровізації.

Інформаційні технології – це сукупність методів, засобів та способів використання сучаних гаджетів для швидкого створення, збору, передачі, пошуку та поширення інформації.

Розглядаючи інформаційні технології зі сторони суспільства, цифровізація публічного управління є інструментом сприяння прозорості та відкритості державних органів.

Діджиталізація – це процес переведення інформації з текстового, звукового чи графічного формату у цифровий формат, зрозумілий сучасним інформаційним пристроям як комп’ютер, ноутбук, телефон чи планшет.

В умовах війни впровадження діджиталізації набуло зовсім іншого рівня. Основним є питання цифрової відбудови, що включає в себе такі проблеми (рис. 1.1):

- відновлення телекомунікаційного забезпечення країни;
- впровадження стратегія розвитку хмарної інфраструктури;
- створення центрів управління кібербезпекою;
- створення електронного архіву та штучного інтелекту для надання адміністративних послуг.

Рис. 1.1 План диджиталізації за переліком газети «Forbes»

Проте, незважаючи на значний потенціал, використання цифрових технологій залежить від політичних, інфраструктурних, соціальних та економічних факторів, як до прикладу:

- Вільний доступ до Інтернет ресурсів;
- Конфіденційна захищеність користувача;
- Доступність для необізнаних людей у цифрових технологій (пенсіонери, люди з обмеженими можливостями, тощо)
- Фінансові витрати задля запровадження в державних органах цифрових систем.
- Порівняно висока оплата послуг з користування певними веб-сайтами та порталами;
- Неможливість використовувати цифрові технології без постійного електропостачання.

Розуміння та правильність трактування вищезазначених понять покладає основу до розуміння взаємодію публічного управління та цифрового суспільства.

2.1 Нормативно-правове регулювання цифровізації у сфері публічного управління

Швидкий розвиток цифровізації обумовлює необхідність нормативно-правового регулювання з боку держави.

Починаючи з 2011 року Україна почала стрімко впроваджувати елементи цифровізації із міжнародного досвіду. Така потреба у негайному впроваджені цифрових технологій спровокувала створення недієвих, безглуздих та гальмівних нормативно-правових актів, які були не зрозумілими як для громадян, так і для службовців.

Відсутність у більшості користувачів можливості придбання техніки, доступу до мережі Інтернет, знань та навичок використання цифрових технологій створювали перешкоди для цифровізації.

На сьогодні питаннями щодо розвитку цифровізації займається Міністерство цифрової трансформації України, що було створене у вересні 2019 року. Міністерство працює над створенням «держави у смартфоні».

До основних цілей можна віднести:

- 100% переведення усіх послуг для суспільства та бізнесу у систему онлайн;

- надати можливість та навчити 6 млн. українців цифровій компетентності;

- підвищи частку ІТ у ВВП країни на 10%;

- забезпечити 95% споживачів високошвидкісним інтернетом.

До основних напрямків діяльності міністерства можна віднести:

1. Взаємодія реєстрів. Інтероперабельність.

Відповідно до Закону України «Про електронні довірчі послуги» інтероперабельність – це технологічна сумісність технічних рішень, що використовуються під час надання електронних послуг, та їх здатність взаємодіяти між собою [19]. Взаємодія різноманітних веб-сайтів, порталів та реєстрів дає можливість до комунікації різних органів державної влади,

судових органів, правоохоронних та інших структур між собою та із суспільством; оптимізації роботи шляхом надання якісних адміністративних послуг через онлайн системи; боротьба із бюрократизмом та корупцією.

Наглядним прикладом є розробка та впровадження електронної системи «Трембіта» – це сучасне організаційно-технічне рішення, яке дозволяє будувати безпечні інформаційні міжвідомчі взаємодії органам державної влади, органам місцевого самоврядування та суб’єктам господарювання через інтернет шляхом обміну електронними повідомленнями між їх інформаційними системами.

Система "Трембіта" є одним із ключових елементів інфраструктури надання електронних послуг громадянам та бізнесу, який забезпечує зручний уніфікований доступ до даних державних реєстрів. [20]

2. Відкриті дані.

У 2016 році Україну було офіційно приєднано до Міжнародної хартії відкритих даних, що містить у собі набір практик та напрямків оприлюднення відкритих даних. Відповідно до Хартії Відкритими називаються оприлюднені цифрові дані з такими технічними і нормативними характеристиками, щоб їх міг вільно використовувати, повторно використовувати та розповсюджувати будь-хто, будь-де і у будь-який час. [21]

Відповідно до ст. 1 Закону України «Про доступ до публічної інформації» публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом. Публічна інформація є відкритою, крім випадків, встановлених законом. [22]

У веб-порталі «Дія» є суб-портал «Дія. Відкритті дані» - центр компетенцій в сфері відкритих даних, що має на меті підвищити рівень знань

про відкриті дані, їх вплив та користь для кожного та допомогти Україні стати однією з найпрозоріших країн світу [23]. Відкритті дані дозволяють кожному відслідковувати будь-яку публічну інформацію через онлайн ресурси у вільному доступі. Важливо зазначити автоматизованість системи опрацювання запитів, а, також, суспільну користь для усіх верств населення та сфер бізнесу.

3. Електронна демократія.

Міністерство разом з міжнародними партнерами здійснює впровадження електронної демократії через ряд інструментів, як, до прикладу:

- *Електронна петиція* – це вільна форма звернення громадян до органів державної влади та органів місцевого самоврядування з вимогою розглянути соціально важливі питання та з проханням вирішення певної проблеми.
- *Електронна консультація* – це збір інформації та різного виду думок та питань, обговорення різного виду рішень, законопроектів та інших нормативно-правових актів в електронній формі.

Дане повноваження регулюється Конституцією України, Законом України «Про звернення громадян», Законом України «Про доступ до публічної інформації», Указ Президента України "Про Порядок розгляду електронної петиції, адресованої Президентові України", Постанова Кабінету Міністрів України "Про затвердження Порядку розгляду електронної петиції, адресованої Кабінету Міністрів України", Розпорядження Голови Верховної Ради України "Про деякі питання забезпечення документообігу у Верховній Раді України в електронній та паперовій формах", а, також, окремі Положення затвердження органами місцевого самоврядування на місцях [22,24-28].

4. Електронна ідентифікація.

Реалії сьогодення потребують для належного впровадження, функціонування та використання інформаційних систем впровадження електронної ідентифікації особи: електронний підпис, BankID, MobileID.

- BankID фунціонує за допомогою даних з українського банку, де громадянин обслуговується. Сервіс надається Національним банком України та можливий лише для клієнтів тих банків, які його підтримують. Перелік постійно оновлюється;
- MobileID функіонує за допомогою оператора мобільного зв'язку, лише за умови, якщо SIM-карта містить електронний підпис. Для отримання такої SIM-карти слід звернутись до вашого мобільного оператора: обміняти наявну SIM-карту на нову та активувати її;
- електронний підпис передбачає використання громадянином електронного підпису (особистого або юридичної особи), який має вигляд окремого файлу або зберігається на захищеному носії чи записаний на ID-картку. Електронний підпис за правовим статусом прирівняний до власноручного підпису або печатки**.**

Це питання регулюється Законом України «Про електронні довірчі послуги», Законом України «Про цифровий підпис». [19].

5. Електронний документообіг.

Запровадження електронного документообігу є важливим кроком впровадження цифровізації в більшості державних органів влади. Розвиток електронного урядування провокує проведення оптимізації створення, збереження та передачі кореспонденції.

Верховною Радою України були прийняті Закони України «Про електронні документи та електронний документообіг», «Про Національну програму інформатизації», «Про телекомунікації», «Про Національну систему конфіденційного зв'язку», «Про захист інформації в інформаційно-телекомунікаційних системах», тощо [29-36].

Закон України «Про електронні документи та електронний документообіг» визначив основні організаційно-правові засади електронного документообігу та використання електронних документів.

6. Мінцифра — регулятор крипто валют.

З 2019 року в Україні офіційно існує поняття віртуальних активів. Віртуальний актив — цифрове вираження вартості, яким можна торгувати у цифровому форматі або переказувати, і яке може бути використане для платіжних або інвестиційних цілей.

Міністерство цифрової трансформації України є регулятором віртуальних активів, розробляє умови ліцензування для постачальників сервісів віртуальних активів та на основі законодавчих актів розробляє алгоритми роботи бізнесу в Україні.

Зовсім нещодавно президент підписав Закон України «Про віртуальні активи».

7. Національна програма інформатизації.

Сфера національної інформатизації регулюється Законом України «Про Національну програму інформатизації».

Відповідно до ст. 2 закону Національна програма інформатизації визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення [31].

Програма спрямована на вирішення таких завдань:

- формування правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних передумов розвитку інформатизації;
- застосування та розвиток сучасних інформаційних технологій у відповідних сферах суспільного життя України;
- формування системи національних інформаційних ресурсів;

- створення загальнодержавної мережі інформаційного забезпечення науки, освіти, культури, охорони здоров'я тощо;
- створення загальнодержавних систем інформаційно-аналітичної підтримки діяльності державних органів та органів місцевого самоврядування;
- підвищення ефективності вітчизняного виробництва на основі широкого використання інформаційних технологій.

«Стратегія цифрової трансформації соціальної сфери», метою якої стало наближення української сфери соціального захисту до європейських стандартів, які включають сучасні інтерактивні технології, новітні інформаційні та управлінські технології, включення стандартів якості обслуговування громадян, з можливістю прийняття ефективних рішень [37]. Також, неабиякою позитивною складовою дотримання стандартів є зменшення рівня бюрократизму та корупції.

Даний проект розрахований на впровадження Єдиної інформаційно-телекомунаційної системи для центрального управління в ІТ сфері враховуючи усі необхідні стандарти. Надання будь-якого виду адміністративних послуг несе за собою рад зобов’язань держави перед громадськістю у вигляді:

- безпеки збереження, обробки та використання інформації;
- швидкості та якості обробки інформації без впливу людських факторів;
- виконання поставлених завдань відповідно до норм чинного законодавства;
- тощо.

Єдина ІТ система зумовлює створення резервів або так званої приватної хмари СУДФ, яка буде в себе включати обчислювальні потужності діючих ЦОД Мінфіну, Держмитслужби, Казначейства, ДПС, Держаудитслужби, Держфінмоніторингу (лише в частині обробки інформації, яка не має грифу обмеження доступу). Саме це є запорукою

безпеки збереження інформації та її дублікації через можливі кібергатаки, збої у системах та інші ситуації, що несуть загрозу знищення інформації.

Створення Єдиної інформаційної системи соціальної сфери повинне включати забезпечення захисту інтересів держави, включаючи передачу у державну власність вихідних кодів (програмних кодів та текстів) на всі елементи програмного забезпечення Єдиної інформаційної системи соціальної сфери, крім тих, що представлено на міжнародному ринку технологій (операційні системи, системи керування базами даних, системи бізнес-аналізу тощо).

Розглянувши показники реалізації Стратегії можна прийти до висновку, що реалізація цієї стратегії здійснюється впровадження Єдиної інформаційної системи соціальної сфери, яка передбачена Стратегією цифрової трансформації соціальної сфери, затвердженою розпорядженням КМУ від 28.10.2020 № 1353-р «Про схвалення Стратегії цифрової трансформації соціальної сфери», постановою Кабінету Міністрів України від 11.11.2020 № 1278 «Про запровадження експериментального проекту з реалізації функціоналів першої черги Єдиної інформаційної системи соціальної сфери».

Провівши моніторинг соціальних мереж Міністерства, на сьогодні, попри початок війни, реалізація стратегії продовжується. За словами заступника Міністра - Костянтина Кошеленко, Міністерство відреагувало на виклики непростої ситуації в країні, продовживши рушити цифровізацію.

«За допомогою впровадження Єдиної інформаційної системи соціальної сфери, а саме її основній частині Єдиному соціальному реєстру стала можлива реєстрація внутрішньо переміщених осіб ще на весні. Пропри значні труднощі у вигляді величезного потоку людей, процес реєстрації став набагато швидшим. Важливо зазначити що Єдина інформаційна система є фундаментом для реалізації соціальних послу. Поступово ця система поповнюється новими видами надання соціальних послуг, а також соціальними допомогами. Єдина інформаційна система спрощує процедуру

подачі документів та заповнення анкет завдяки взаємодії з різними державними реєстрами. Ця програма покликана об’єднати усі органи соціального захисту. Цифровізація під час війни – це не лише про комфорт громадян, а й про їх безпеку» - зауважив пан Костянтин у вищезазначеному інтерв’ю [51].

Таким чином, попри складну ситуацію в країні, держава стрімко проходить етапи становлення цифровізації та регулює їх за допомогою впровадження нових та ефективних нормативно-правових актів.

РОЗДІЛ 2. АНАЛІЗ ШЛЯХІВ ТРАНСФОРМАЦІЇ ДІЯЛЬНОСТІ АНТИМОНОПОЛЬНОГО КОМІТЕТУ В УМОВАХ РОЗВИТКУ ЦИФРОВОГО СУСПІЛЬСТВА

2.1 Дослідження інструментів трансформації органів публічних органів в умовах цифрового суспільства на прикладі Антимонопольного комітету України.

Не є секретом, що саме Революція Гідності стала сильним поштовхом до кардинальної реформації влади. Беручи до уваги створення демократичної держави слідує такий шлях її реалізації: держава та громадяни створюють певну діалектичну єдність, що зумовлена розвитком різних галузей діяльності держави.

Демократична та правова держава залежна від розвитку громадського суспільства. Особливість існування демократичної держави та суспільства ґрунтується на довірі громадян та контролю за діяльністю влади.

На сьогодні, із впровадження цифрових технологій держава стала набагато ближчою до громадянина. Існує чимало засобів комунікації органів державної влади і суспільства:

- веб-сайти органів державної влади;
- е-петиції, е-звернення, е-консультації;
- моніторинги, опитування, анкетування;
- Інтернет платформи;
- «гарячі» та «прямі» телефонні лінії;
- інші засоби.

Державні органи влади все більше залучають громадськість до творення державної політики чим прискорюють адаптацію цифровізації у державі.

На прикладі вивчення інструментів взаємодії Антимонопольного комітету України у особі Південно-західного Відділення проведено аналізу основного веб-сайту Комітету та суб-сайту Відділення.

Веб-сайт – це віддзеркалення душі структури, підприємства, організації, тощо. За допомогою веб-сайту будь-яка людина може відшукати необхідну інформацію для себе без її фізичної присутності у Відділені.

Також сайт – це перша інформаційна платформа, де можливо дізнатись місце знаходження структури та усю контакту інформацію.

Під час здійсненя дослідження я звернула увагу на те, що до 2020 року сайт мав зовсім інший вигляд, був застарілим відповідно до умов сучасності та неактуальним для користувачів (рис. 2.1).

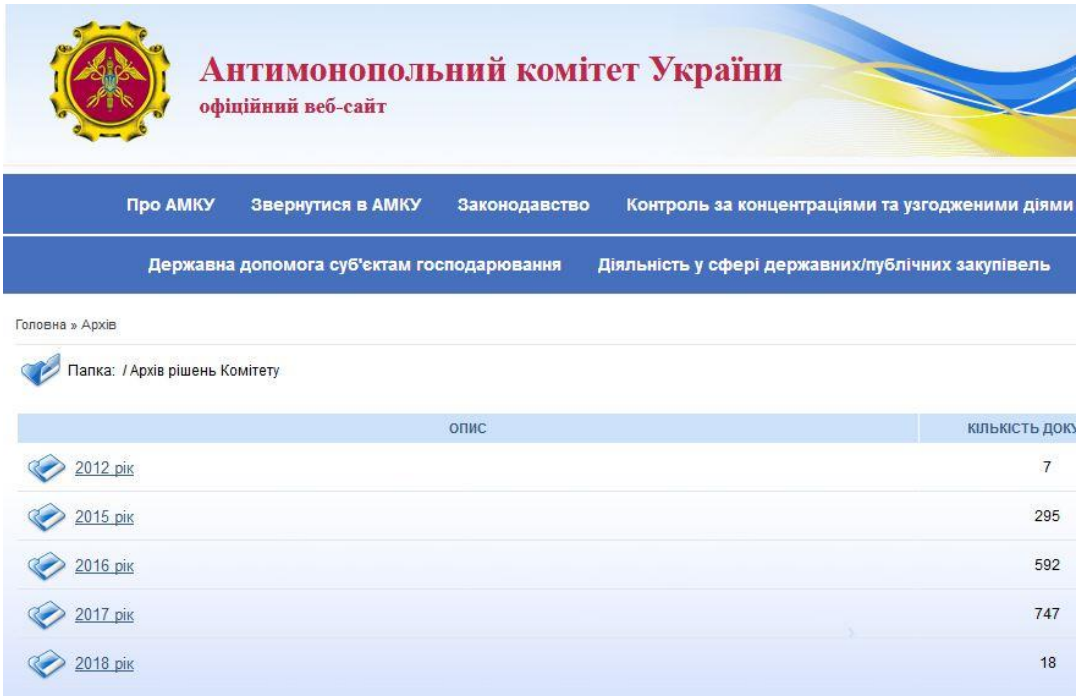


Рис. 2.1 – Веб-сайт Антимонопольного комітету України у 2019 році

Відповідно до наданого рисунку, сайт виглядав не зрозуміло, вкладки були не розділеними та втрачався фокус користувача.

Для того аби знайти більш детальну інформацію неохідно заходити по безлічі вкладок. Функція «Пошук» не мала достатнього розширення для швидкого та якісного пошуку інформації.

У 2020 році Антимонопольний комітет України змінив сайт повністю.

Новий дизайн та лаконічне оформлення позитивно впливає на користувачів. Уся первинна інформація знаходиться на головній сторінці (рис. 2.1.2). [52]

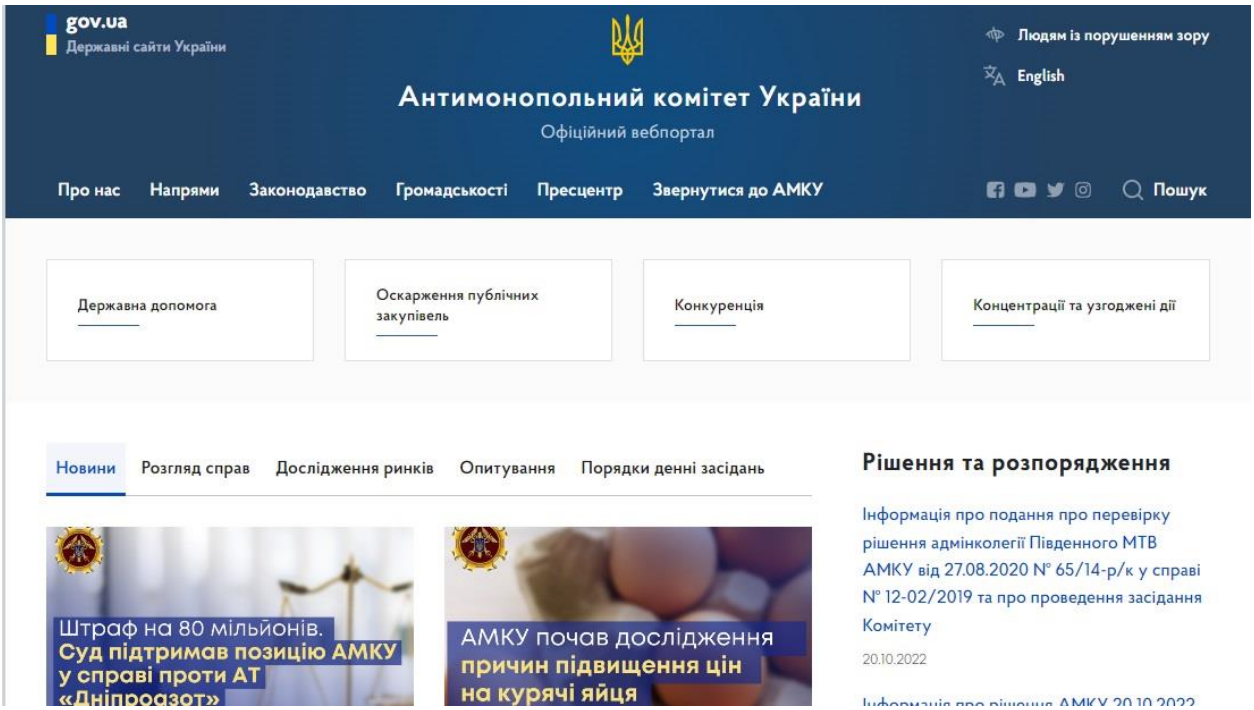


Рис 2.2 – Головна сторінка Веб-сайту Антимонопольного комітету України після зміни у 2020 році

Новини є актуальними, а, також, можна знайти інформацію щодо розгляду справ, досліджень на ринку, різноманітних опитувань та інформацію щодо засідань адміністративної колегії Відділення.

Чудовим вкладом є рубрики «Найближчі події» з коротким описом події та її датою, розділ «Вакансії» де ти можеш знайти умови конкурсу на певну посаду, а також накази про призначення (рис. 2.3).

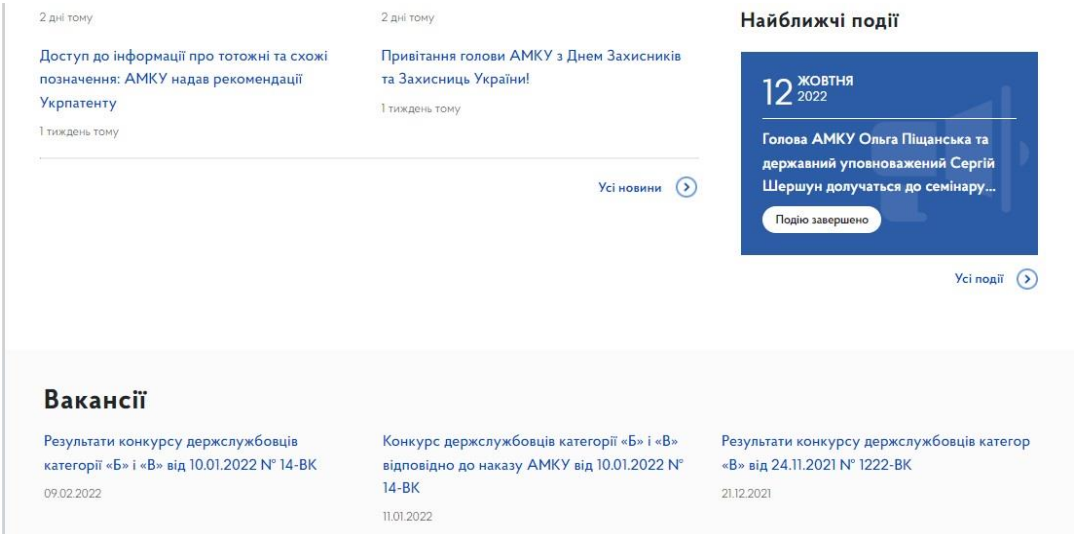


Рис. 2.3 – Рубрики «Найближчі події» та «Вакансії»

Також є розділ із «Корисними посиланнями» такими як :

- Тетування та навчання з української мови;
- Дія. Платформа центрів;
- Безоплатна правова допомога;
- Телефони гарячих ліній;
- Тощо. (рис. 2.4).

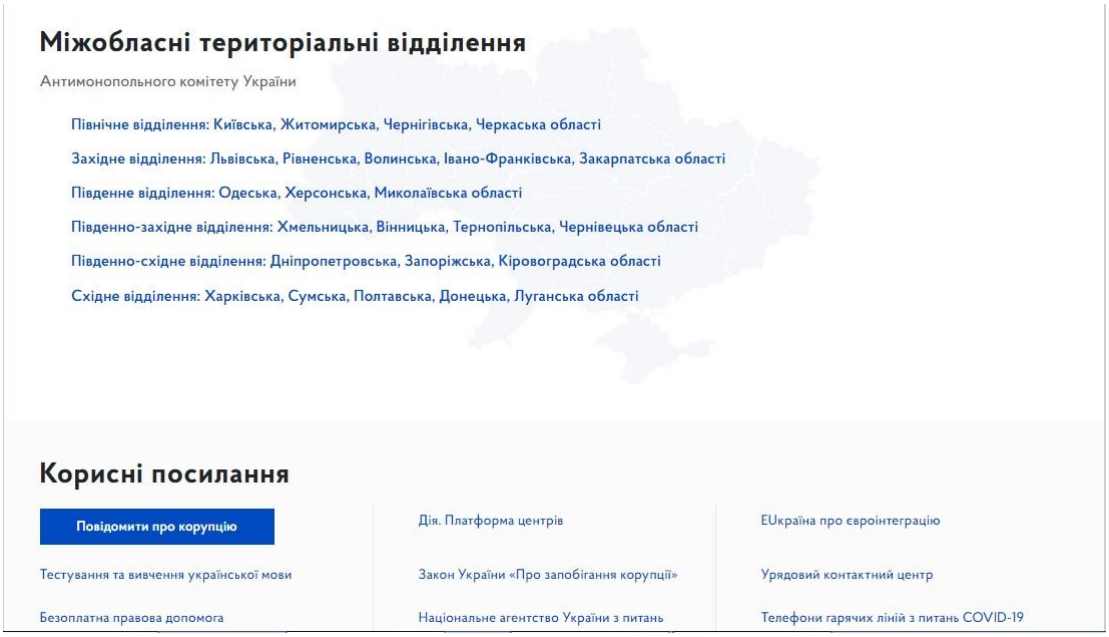


Рис. 2.4 – Рубрики з переліком суб-сайтів Віддіень Антимонопольного комітету України та корисними посиланнями.

Для зручності через головну сторінку Антимонопольного комітету України є посилання на реформовані у 2020 році Відділення з розписом областей, які до них входять.

Також, для людей із порушенням зору є окремий режим для зручності у користуванні сайту, що є неабиякою запорукою доступу до інформації. (рис. 2.5).

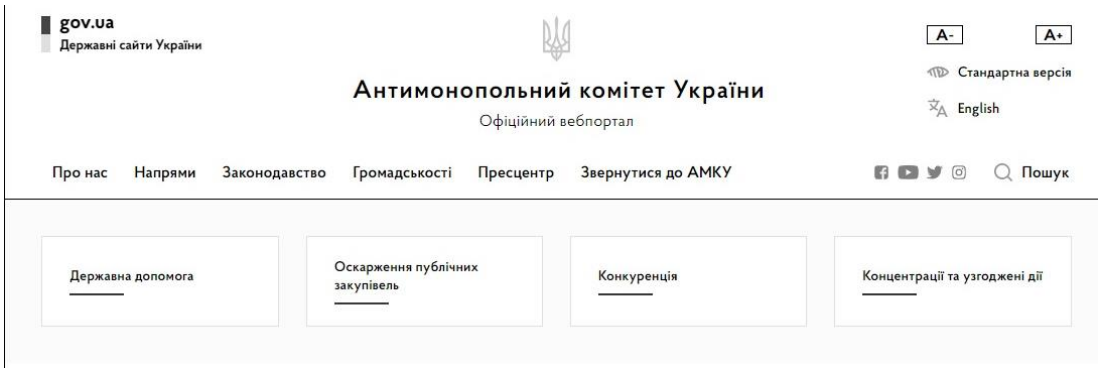


Рис.2.5 – Вигляд сайту із включенням фунції для людей із порушенням зору.

Суб-сайти Відділень є складовою частиною загального сайту Антимономольного комітету України, проте вміщають у собі більш детальну інформацію по обостях. (рис. 2.6).

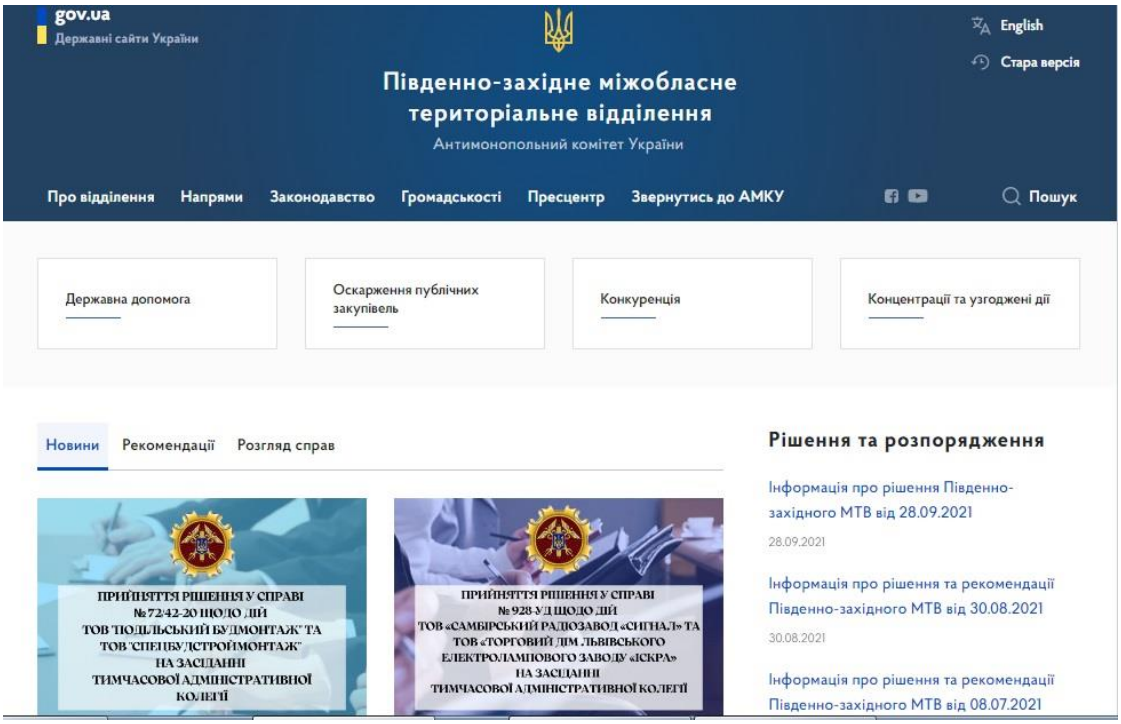


Рис. 2.6 – Головна сторінка суб-сайту Південно-західного міжобласного територіального відділення Антимонопольного комітету України.

За останні 3 роки суб-сайт став доступнішим, більш відкритим та наповненим.

Користувачеві досить легко шукати необхідну інформацію, роздрукувати її через пряму систему друку без копіювання, знайти інформацію по словах «маркерах» не лише у внутрішніх документах, а і у НПА в цілому.

Модернізація суб-сайту є складовою приближення Антимонопольного комітету України до вимог цифрового суспільства.

Звернення громадян через подачу е-петицій та е-звернень.

Портал відкритих даних (data.gov.ua) – це онлайн платформа, що містить у собі велику кількість публічної інформації для загального користування [40].

Пошук інформації відбувається за розпорядниками інформаціями, групами, ліцензіями, форматами документів та ключовими словами.

На платформі є цікаве вкладення як «Аналітика» (рис. 2.7).

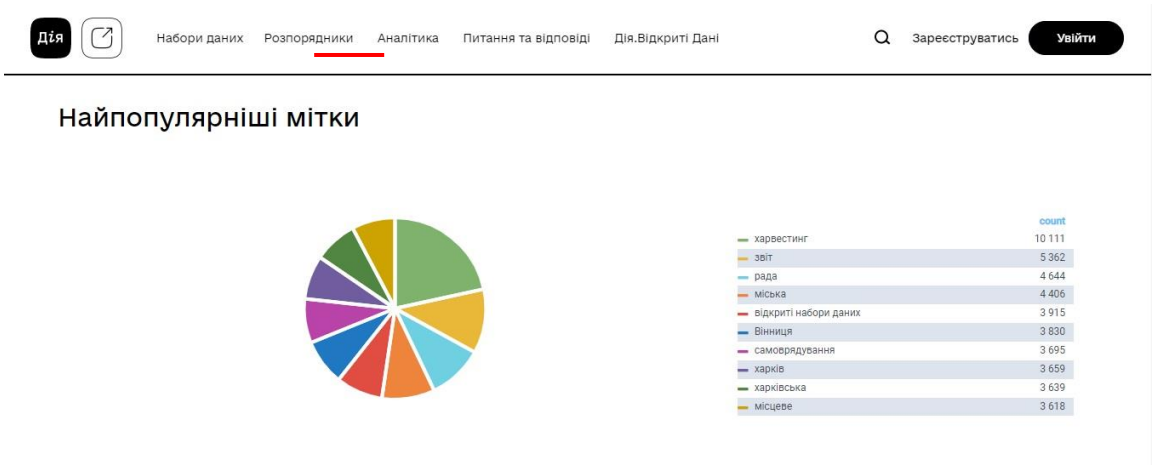


Рис. 2.7 – Найпопулярніші мітки для пошуку інформації на Порталі відкритих даних

На цій сторінці розмішені статистичні дані щодо найпопулярніших запитів, міток, частоти оновлення інформації, динаміка росту кількості публікації інформації.

Також, важливою вкладкою є розділ «Питання та відповіді»» (рис. 2.8).

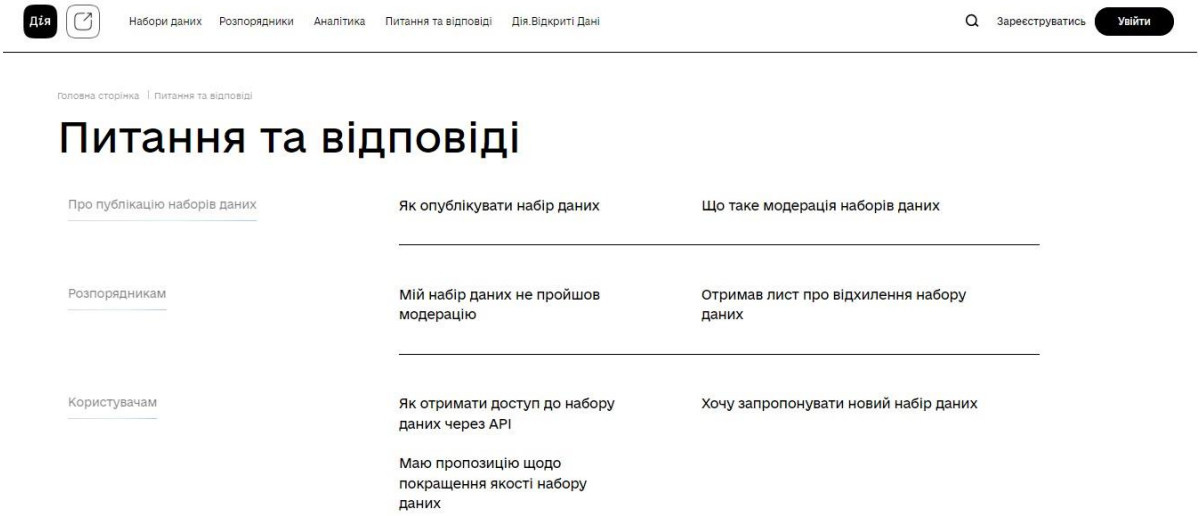


Рис. 2.8 – Рубрика «Питання та відповіді»

Чудовим рішенням є розподіл питань та відповідей для різних користувачів порталу, а, також, підбір найактуальніших питань.

Розміщення публічної інформації органими державної влади є свідоме слідування нормам чинного законодавства, в тому числі Закону України «Про доступ до публічної інформації» та підвищення рівня довіри

суспільства до держави, як сторінка Антимонопольного комітету України (рис. 2.9).

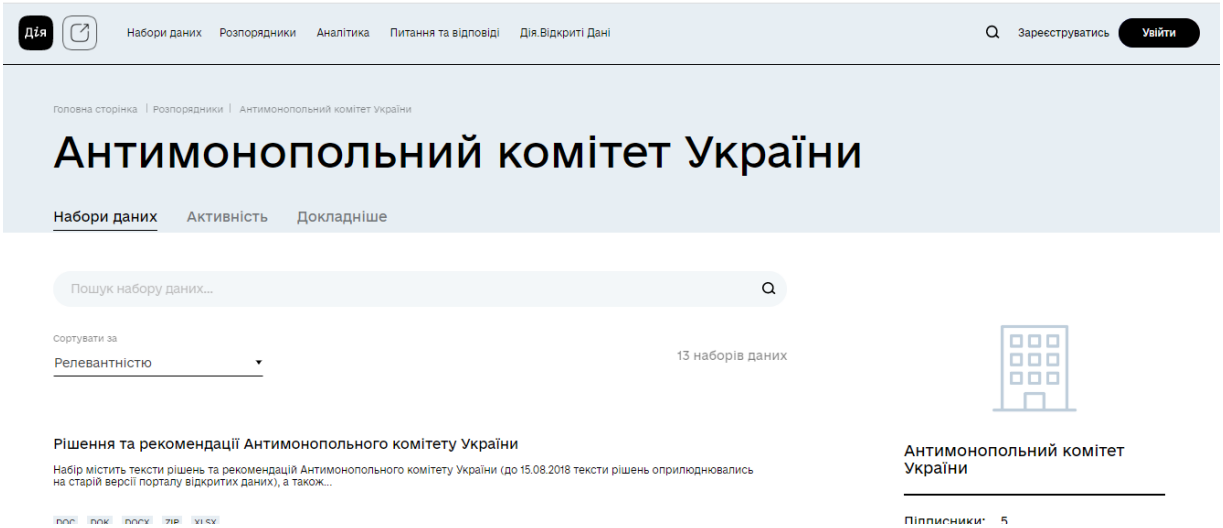


Рис 2.9 – Сторінка Антимонопольного комітету України на Порталі відкритих даних

Дія. Відкритті дані – це центр компетенцій, що допомагає користувачеві підвищити рівень знань стосовно відкритих даних та їх суспільну користь. Це прагнення створити та використовувати центр для побудови насправді відкритої та прозорої держави для громадянина.

Одним із найважливішим аспектом взаємодії громадянина та органів державної влади є звернення громадян.

Відповідно до Закону України «Про звернення громадян» кожен громадянин, або особа без громадянства, яка законно проживає на території України, має право звернутися до органів державної влади, місцевого самоврядування, об’єднань громадян, підприємств, установ, засобів масової інформації, посадових осіб відповідно до наділених повноважень та обов’язків із скаргою, заявою чи пропозицією щодо реалізації чи порушення своїх соціальних, політичних, економічних прав [25].

Із впровадженням цифровізації досить популярним стало подання електронної петиції та електронної консультації.

Електронна петиція – це вільна форма звернення громадян до органів державної влади та органів місцевого самоврядування з вимогою розглянути соціально важливі питання та з проханням вирішення певної проблеми [49].

Кожен громадянин може ініціювати власну е-петицію, а розгляд є обов'язковим після збору достатньої кількості підписів інших громадян на офіційних веб-сайтах органу влади чи громадського об'єднання (рис. 2.10).

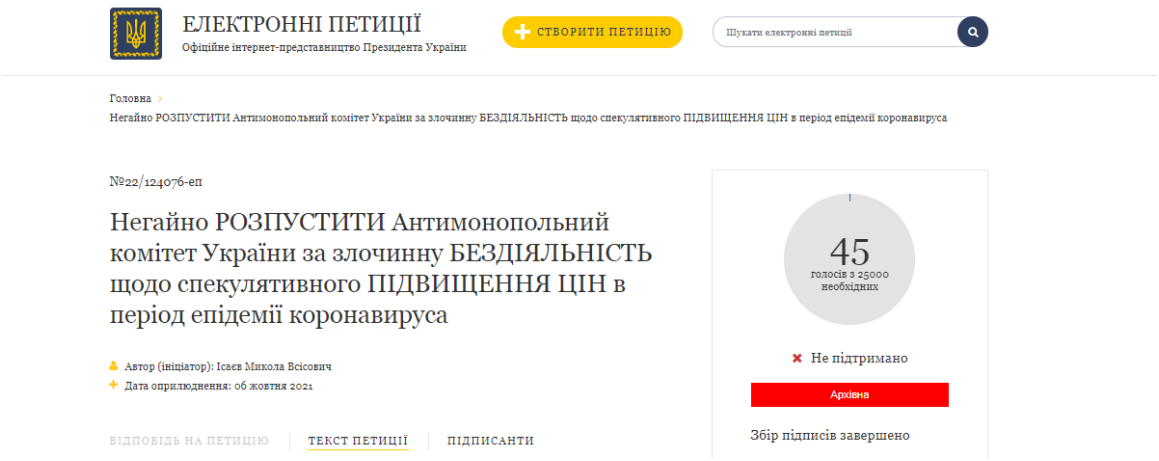


Рис. 2.10 – Електронна петиція про розпуск Антимонопольного комітету України.

Значними перевагами електронної петиції є відкритість та зручність розміщення петиції в електронному варіанті без фізичної необхідності збору підписів, ефективність поширення інформації та залучення більшої кількості громадян (Рис. 2.11)

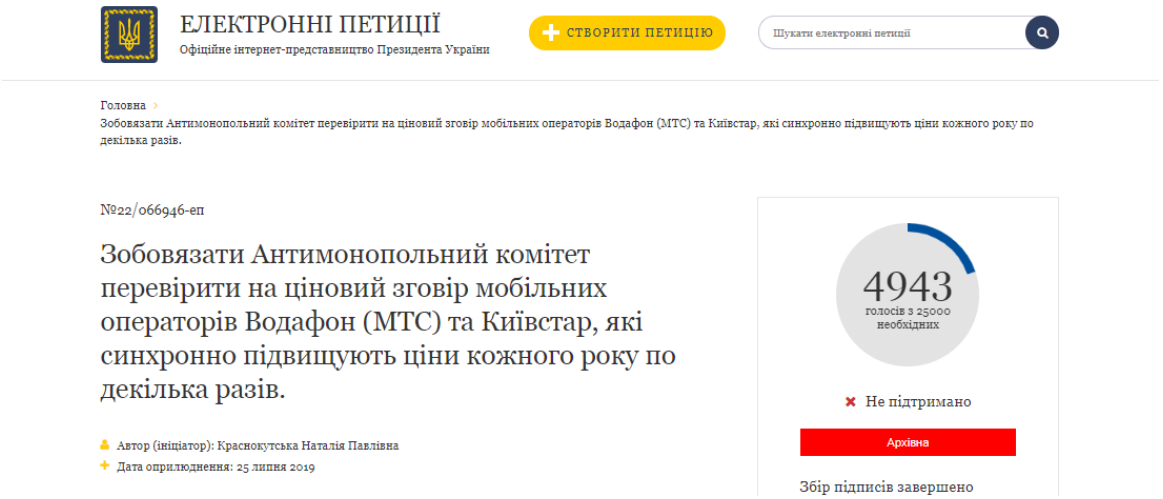


Рис. 2.11 – Електронна петиція щодо зобов'язань перевірки Антимонопольним комітетом України провайдерів телефонного зв'язку.

В електронній петиції має бути викладено суть звернення, зазначено прізвище, ім'я, по батькові автора (ініціатора) електронної петиції, адресу електронної пошти. На веб-сайті відповідного органу або громадського об'єднання, що здійснює збір підписів, обов'язково зазначаються дата

початку збору підписів та інформація щодо загальної кількості та переліку осіб, які підписали електронну петицію.

Також, через свій онлайн формат з е-петицією можуть ознайомитись не лише пересічні громадяни, а й представники ЗМІ, державні службовці, депутати та інші уповноважені особи ще до повного збору підписів.

Електронна консультація – це збір інформації та різного виду думок та питань, обговорення різного виду рішень, законопроектів та інших нормативно-правових актів в електронній формі**.**

Існують різні види консультацій: формальні, неформальні, регульовані державою та не регульовані. Дана форма електронної демократії було законодавчо закріплена Постаною Кабінету Міністрів України «Про затвердження порядоку проведення консультацій з громадськістю з питань формування формування та реалізації державної політики», а також, окремо затвердженими Порядки на рівні органів місцевого самоврядування.

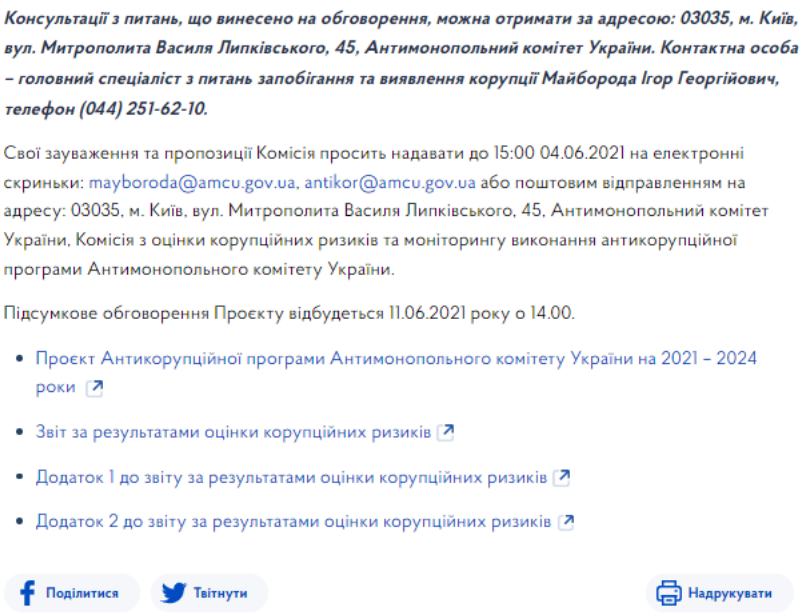
Антимонопольний комітет України пропонує для громадського обговорення різні проекти, як наприклад, проведення опитувань споживачів під час розгляду справ про порушення законодавства про захист економічної конкуренції (про захист від недобросовісної конкуренції), дослідження ринків.

Зокрема, цей електронна консультація допомагає визначити:

- мету та основні принципи проведення різного виду досліджень у справі;
- процедуру організації проведення досліджень у справі;
- основні етапи та порядок проведення досліджень у справі;
- вимоги до досліджень у справі;
- тощо.

Антимонопольний комітет України закликає представників громадськості, експертного середовища, бізнесу та інші заінтересовані сторони ознайомитися з документом. Зауваження та пропозиції до проектів

можливо надсилати протягом 30 днів з дня їх оприлюднення на веб-сайті (рис. 2.12)



Консультації з питань, що винесено на обговорення, можна отримати за адресою: 03035, м. Київ, вул. Митрополита Василя Липківського, 45, Антимонопольний комітет України. Контактна особа – головний спеціаліст з питань запобігання та виявлення корупції Майборода Ігор Георгійович, телефон (044) 251-62-10.

Свої зауваження та пропозиції Комісія просить надавати до 15:00 04.06.2021 на електронні скриньки: mayboroda@amcu.gov.ua, antikor@amcu.gov.ua або поштовим відправленням на адресу: 03035, м. Київ, вул. Митрополита Василя Липківського, 45, Антимонопольний комітет України, Комісія з оцінки корупційних ризиків та моніторингу виконання антикорупційної програми Антимонопольного комітету України.

Підсумкове обговорення Проєкту відбудеться 11.06.2021 року о 14.00.

- Проєкт Антикорупційної програми Антимонопольного комітету України на 2021 – 2024 роки
- Звіт за результатами оцінки корупційних ризиків
- Додаток 1 до звіту за результатами оцінки корупційних ризиків
- Додаток 2 до звіту за результатами оцінки корупційних ризиків

Поділитися Твітнути Надрукувати

Рис. 2.12 Інформація розміщене на сайті Антимонопольного комітету України щодо е-консультацій.

У сферу діяльності Антимонопольного комітету України входить робота та перевірка діяльності суб’єктів господарювання пов’язаної із тендерними закупівлями. Найбільш зручними та популярними є офіційні майданчики електронної системи публічних закупівель України «ProZorro», «Е-Тендер», «Держзакупівлі.Онлайн», «Смарттендер» та «Закупки.пром.уа». [41-44].

Ідея тендеру полягає у прояві чесної конкуренції на ринках послуг. Але попри досить позитивний задум створення прозорих торгів, часто спостерігається приховані задуми із порушенням законодавства.

Електронні торги є сучасним та зручним форматом співпраці замовника послуг і продавця. Це виражається в прозорості вимог всіх учасників, доступ без кордонів за наявності мережі Інтернет, анулювання корупційних схем та створення конкурентних діалогів, нижча вартість, ніж оплата рекламних послуг, а, також, можливість оскарження торгів, що є сумнівними у Антимонопольному комітеті України шляхом написання заяви про порушення законодавства про захист економічної конкуренції.

Усі цифрові інструменти, що використовує Антимонопольний комітет України є дієвими засобами на шляху трансформації органу в умовах цифрового суспільства.

2.2 Оцінка рівня трансформації органів публічного управління в умовах цифрового суспільства на прикладі Антимонопольного комітету України.

У дослідженні найважливішим аспектом стало вивчення готовності державної служби до вимог цифрового суспільства. Дане питання є надзвичайно актуальним та проблематичним, адже впровадження цифрових технологій і діяльність державних органів є необхідністю для реалізації ідеї «цифрової держави». Враховуючи сучасну модель державної служби за останні 3 роки майже усі послуги, реєстри, діловодство, підвищення кваліфікації та інші аспекти роботи державного службовця відбуваються через цифрові технології.

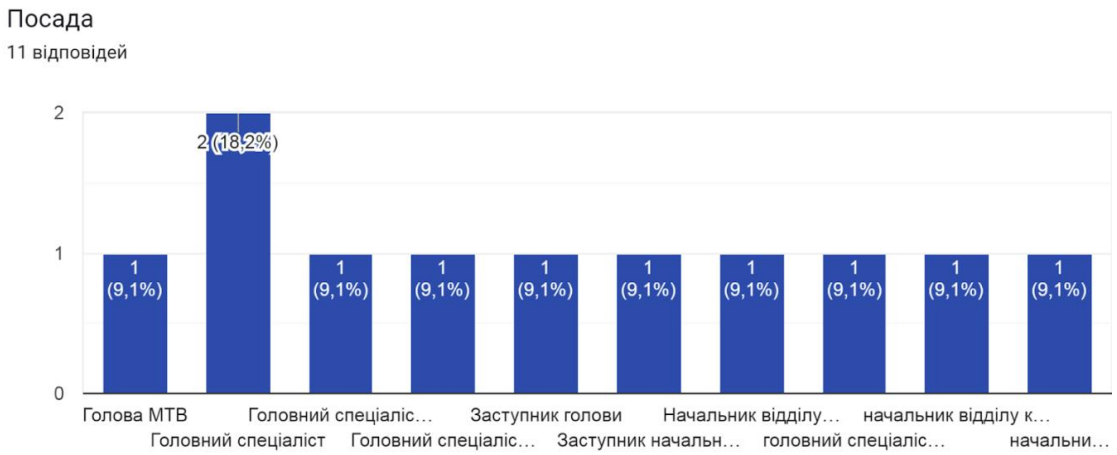
Проте, важливо зауважити, що цифровізація державної служби неможлива без відповідної кваліфікації працівників та їх готовності до вимог цифрового суспільства.

Орієнтованість та використання ІТ технологій є запорукою злагодженої роботи держави та суспільства у аспекті комунікації, а також демонстрацією рівня розвитку демократичної та передової держави. На сучасному етапі розвитку цифрового суспільства цифрова грамотність як державного службовця, так і громадянина є першочерговою вимогою до здійснення цифровізації.

Під час проведення дослідження було розроблено тестування через програму Google Forms для працівників Південно-західного міжобласного територіального відділення Антимонопольного комітету України щодо оцінки цифрової компетентності державного службовця до вимог цифрового суспільства.

Тестування складалося із таких запитань:

1. **Посада** – це запитання є стандартним і розраховане на оцінку компетентності в залежності від обов’язків державного службовця (діаграма 2.1).



Діаграма 2.1 - Посада

У опитування взяли участь різні категорії державних службовців із різними посадами та різними аспектами роботи:

- Голова Відділення;

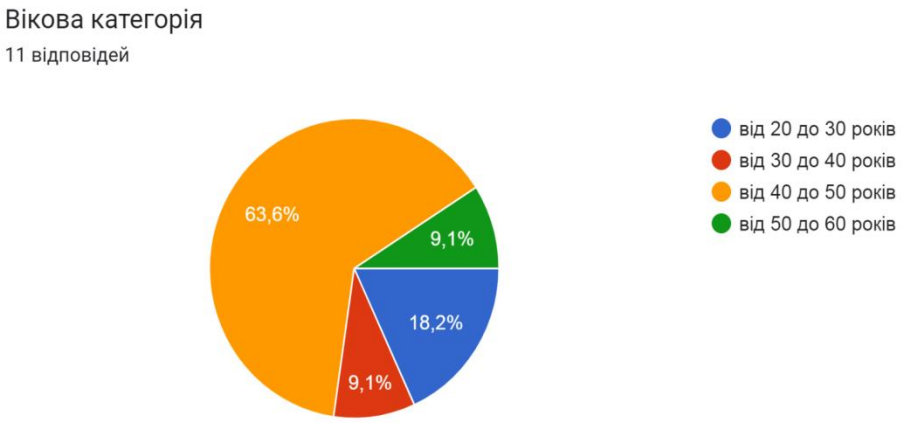
- Заступник голови Відділення;

- Начальники Відділів;

- Головні спеціалісти відділів.

Важливе місце мало задіяти максимальну кількість фахівців та оцінити їх знання у цифровізації.

2. Вікова категорія – це запитання розраховане на співвідношення віку із зняннями цифрових технологій. Також варто зазначити що відповідно до результатів найбільший відсоток працівників віком від 40 до 50 років (діаграма 2.2) .

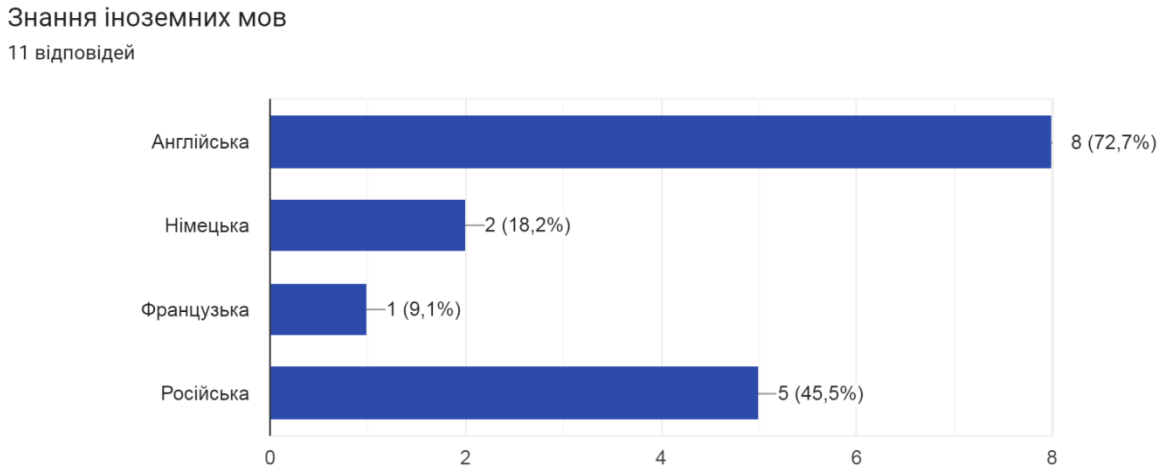


Діаграма 2.2 – Вікова категорія

Цей факт дозволяє зробити висновок, що вік не є перепоною для здобуття знань з користування інформаційними технологіями. Хоча існує стереотип, що старше покоління дуже важко адаптується до вимог цифрового суспільства та із складнощами здобувають цифрову компетентність, у реаліях все залежить від бажання навчатись та реалізації службою умов та можливостей для здобуття необхідної цифрової компетентності.

3. Знання іноземних мов – це питання є актуальним для будь-якої особи. На сьогодні багато веб-сайтів, програм та інших інформаційних систем побудовані на іноземній мові. Важливо розуміти елементарні речі, а також, задля комунікації із міжнародними партнерами, важливо мати знання із іноземних мов. Нещодавно у Південно-західному міжобласному відділенні Антимонопольного комітету України та за участі представників інших Відділень і Центрального Апарату відбулася веб-конференція щодо створення презентацій, ведення публічних виступів та оформленні подачі інформації для різного виду зустрічей, нарад та заходів адвокатування. Веб-конференція відбувалася у онлайн формі, а лекторами виступали представники державної служби із Литви, Польщі та Румунії. Лекція відбувалася у формі діалогу та проводилася виключно англійською мовою.

За результатами опитування більшість опитуваних володіють англійською мовою (Діаграма 2.3).



Діаграма 2.3 – Знання іноземних мов

Нещодавно голова Національного агентства з питань держаної служби повідомила про можливі нові вимоги для працівників державної служби: знання права Європейського союзу і його інституцій та володіння англійською мовою.

Проте, варто зауважити, що для ефективності впровадження таких змін до вимог працівника державної служи необхідне заохочення працівника до проходження начання. Тому у кожного державного службовця незабаром буде можливість безкоштовного вивчення іноземної мови за програмами найбільшої у світі освітньої організації EF (Education First) Language Learning Solutions. Реалізація цього амбітного плану є неабиякою запорукою інтеграції України до Європейського союзу та несе масу корисних можливостей для розвитку державної служби в Україні.

4. Портали (сайти) якими користуються державні службовці – це питання складається із переліку найбільш популярних та необхідних у роботі працівників Відділення порталів та сайтів.

Варто зазначити, що різні категорії працівників використовують лише необхідні для роботи інформаційні системи. Проте, для належного використання, необхідно вміти правильно шукати та використовувати інформацію.

Відповідно до відповідей на дане питання найбільше використовують Офіційний портал Верховної ради України – 100% опитаних працівників (Діаграма 2.4).

Діаграма 2.4 – Портали та сайти для користування

Проте для кожної категорії працівників та їх кола обов'язків використовуються наступні найбільш необхідне системи, портали та сайти:

Для юридичного відділу – електронний суд, де можливо знайти необхідні рішення суду, ухвали та постанови, що справ у різних судах за категоріями: назва суду, суддя, номер справи, кваліфікація порушення, тощо.

Для сектору організаційної роботи (діловодства) – система електронного документообігу АСКОД, за допомогою якої відбувається швидка реєстрація документів та їх підписання цифровим підписом, що дозволяє оперативно знайти інформацію, надіслати за необхідності та з точки зору екології менше використовувати папір для друку.

Для спеціалістів відділів досліджень та розслідувань - офіційні майданчики електронної системи публічних закупівель України як «ProZorro», «Е-Тендер», «Держзакупівлі.Онлайн», «Смарттендер» та «Закупки.пром.уа», суб-сайти органів місцевого самоврядування, підприємств, організацій та інших суб'єктів господарювання, де можливо знайти усю необхідну інформацію щодо їх діяльності для проведення досліджень у справах.

5. Використання електронного цифрового підпису – це питання має за мету оцінку навичок та сфер використання цифрового підпису державним службовцем.

Нагадаємо, на сьогодні, використання електронного цифрового підпису спостерігається при користуванні майже усіма адміністративними послугами,

а відповідно до норм чинного законодавства електронний цифровий підпис має таку ж юридичну силу, як і «живий» підпис особи.

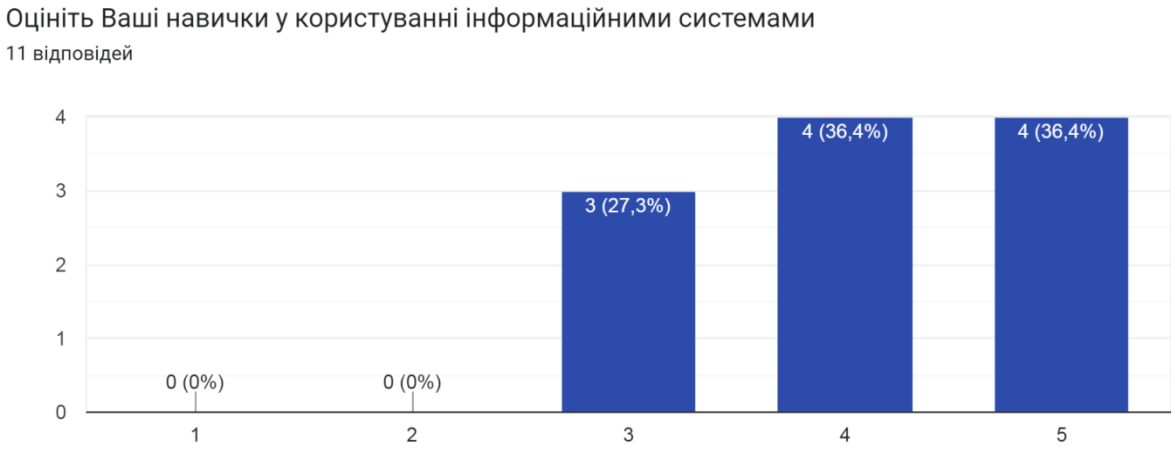
Оцінка відповідей дає змогу зробити висновок, що максимальний відсоток працівників використовує електронний цифровий підпис не лише в робочих цілях для підпису документів, а й у повсякденному житті – 45, 5% (Діаграма 2.5).

Діаграма 2.5 – Використання цифрового підпису

Проте, важливо зазначити, що таких несуттєвих 10% працівників демонструє, що існує певна проблема використання цифрового підпису – не знають як використовувати цифровий підпис, а, також, є працівники які знають про дію цифрового підпису, але не вміють використовувати його.

Багато науковців та користувачів електронним цифровим підписом схиляються до думки, що використання ЕЦП є одним надзвичайно дієвих засобів у боротьбі із бюрократизмом.

6. Оцінка навичок у користуванні інформаційними системами – це питання орієнтоване на власну оцінку державного службовця виходячи із аспектів його роботи та виконання ним обов’язків із повним використанням цифрових технологій (діаграма 2.6).

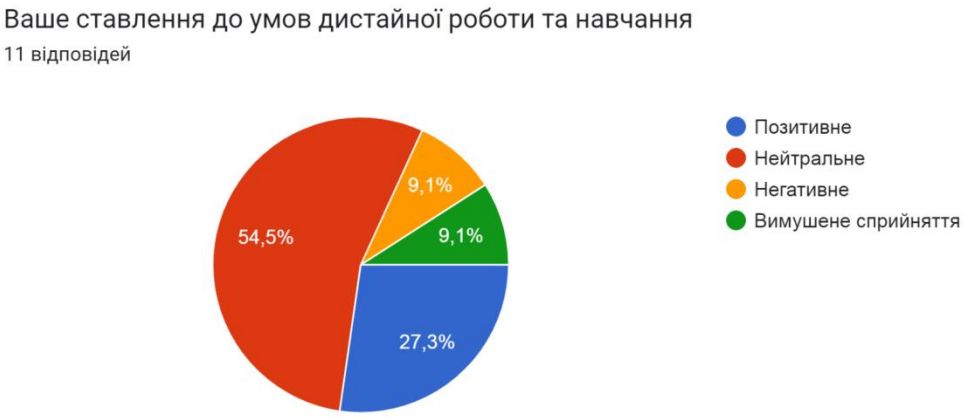


Діаграма 2.6 – Навички у користування інформаційними системами

Проаналізувавши відповіді можливо зробити висновок що лише 36,4% опитаних працівників оцінюють власні навички на високому рівні, інші не є досить компетентними. Проте, у чому ж вимірюється компетентність?

Важливим є не лише повне використання інформаційних систем, але й швидкість пошуку інформації, вміння опрацьовувати та відфільтровувати інформацію, правильно ставити питання, використовувати фільтри та слова «маркери», а також розмежовувати правдиву інформацію від недостовірної. Набуття цих навичок напряму залежать від знань та практики особи.

7. Ставлення до умов дистанційного навчання – це питання спрямоване до визначення думок державних службовців до дистанційної форми навчання, яка набула піку популярності під час введення карантинних обмежень, а сьогодні, воєнного стану(діаграма 2.7).



Діаграма 2.7 – Ставлення до умов дистанційної роботи та навчання.

Проте думки суттєво різняться. Відповідно до аналізу відповідей працівників найвищий відсоток працівників нейтрально відносяться до дистанційного навчання – 54,5% опитаних.

Проте є відсоток осіб, які ставляться негативно, через вимушеність проходження лише дистанційного навчання без альтернативи, халатного відношення до слухання та обговорення, відсутність фізичного контакту та атмосфери навчання.

Після проведення опитування працівників Південно-західного міжобласного територіального відділення Антимонопольного комітету України проведено SWOT-аналіз навчання через платформу «Дія. Цифрова освіта» (таблиця 2.1)

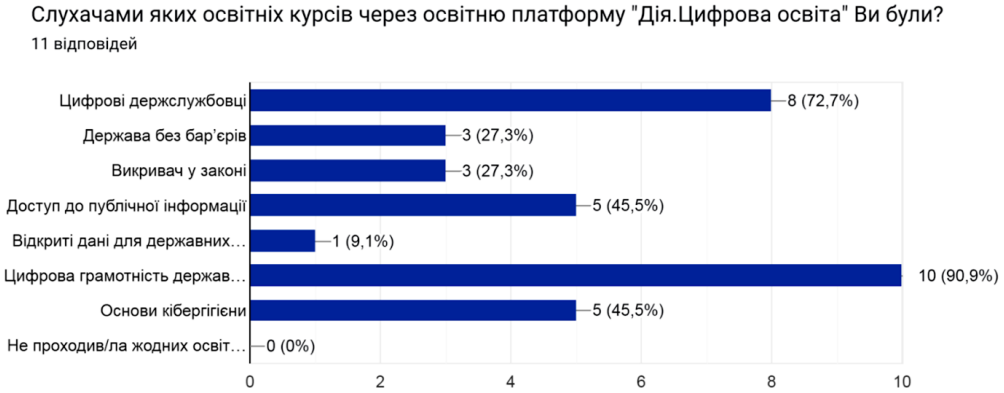
СИЛЬНІ СТОРОНИ	**СЛАБКІ СТОРОНИ**
❖ Навчання проводиться на безоплатній основі; ❖ Можливість навчатись у будь-який час; ❖ Вільний вибір матеріалу для вивчення; ❖ Мобільність начання за допомогою смартфонів, ноудбуків, компютерів та планшетів.	❖ Відсутність вербального контакту між студентами та лектором; ❖ Слабка мотивація до навчального процесу; ❖ Вміння працювати з різномінітними цифровими технологіями; ❖ Виклад матеріалу виключно через електронні носії.
МОЖЛИВОСТІ	**ЗАГРОЗИ**

❖ Економія власного часу через вибір приорітетних напрямків навчання; ❖ Підвищення кваліфікації різних категорій користувачів у вільному доступі; ❖ Економія власних заощаджень; ❖ Залучення величної кількості навчальних матеріалів; ❖ Можливість поєднувати навчання та роботу.	❖ Зловживання користувачами дистанційним навчанням та перехід з денної форми навчання до дистанційного на повній основі; ❖ Зниження ефективності навчального процессу; ❖ Упущення важливих фактів навчання та неуважніть користувачів; ❖ Неможливість навчання через відсутність інтернет-ресурсів, електроенергії або технічних засобів.

Таб. 2.1 - SWOT-аналіз навчання через платформу «Дія. Цифрова освіта».

Ці дані свідчать про готовність працівників навчатись як з фізичною присутністю, так і дистанційно. Варто також підкреслити, що 27,3% - ставляться позитивно.

8. Освітні курси через платформу «Дія. Цифрова освіта» - питання щодо проходження освітніх курсів через платформу «Дія. Цифрова освіта» є надзвичайно цікавим. Відповідно до опитування усі працівники проходили курси (діаграма 2.8).



Діаграма 2.8 – Які навчальні освітні курси проходили працівники.

Найпопулярнішими освітніми серіалами є «Цифрова грамотність державного службовця 1.0» - 90,9 % та «Цифрові держслужбовці» - 72,7%,

що дозволяють опанувати з нуля основні аспекти цифрових технологій, покладаючи основу цифровізації державної служби.

9. Нормативно-правові акти, якими регулюється питання цифровізації – питання, яке демонструє орієнтованість державного службовця у законодавчій основі цифровізації, що невпинно збільшується.

Законодавче регулювання на рівні держави є запорукою правильності, швидкості та якості проведення наближення та поступовій відповідності державної служби до вимог цифрового суспільства.

Відповідно до результатів, не усі державні службовці вільно володіють навіть основними нормативно-правовими актами регулювання впровадження та діяльності цифрових технологій (діаграма 2.9).

Діаграма 2.9 – Оцінка обізнаності в нормативно правовому регулюванні цифровізації.

10. Способи здобуття нових знань та навичок цифрової компетентності – питання спрямоване на дослідження різних способів для навчання та визначення найефективнішого з точки зору державного службовця.

Оцінюючи відповіді можливо виділити, що самоосвіта є найкращим спосіб здобуття цифрової компетенції – 100% (діаграма 2.10). Можливо дійти до логічно висновку, що державні службовці мають бажання більше самостійно вивчати нові аспекти цифровізації, отримувати навички та знання, які їх необхідні та за власним вибором.

Діаграма 2.10 – Способи здобуття цифрової компетентності.

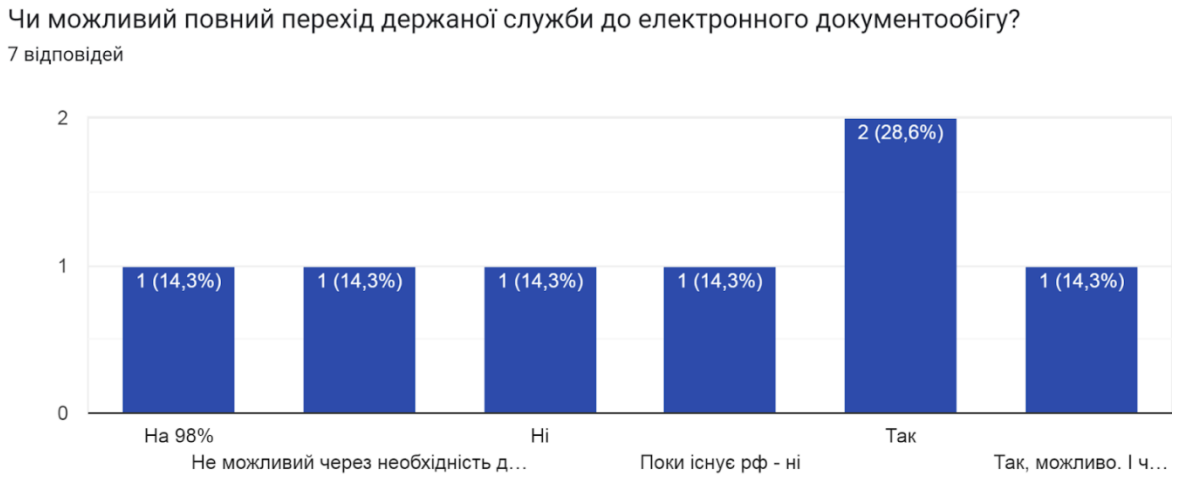
11. Яка бачення поняття цифрове суспільство є у державного службовця – питання, яке спрямоване на визначення поняття цифрового суспільства з точки зору досвідчених державних службовців.

На думку працівників цифрове суспільство – це:

- продуктивне використання цифрових технологій;
- широке використання ІТ технологій у всіх сферах суспільного життя;
- використання цифрових технологій для власних потреб (самореалізація), для роботи, навчання, дозвілля, а також для досягнення та реалізації спільних економічних, суспільних та громадських цілей;
- суспільство, яке йде в ногу з цифровими технологіями;
- зручність і безпека;
- використання цифрових технологій в усіх сферах життя;
- впровадження цифрових технологій в усіх сферах суспільного життя, а саме для власних потреб, робити, відпочинку, навчання тощо;
- використання цифрових систем в усіх аспектах життя.

Важливо зазначити, що думки сходяться у тому, що це використання цифрових технологій в усіх аспектах життя, і є працівники, які повноцінно відповіли на задане питання.

12. Найбільш актуальне є останнє запитання «Чи можливий повний перехід держаної служби до електронного врядування?» (діаграма 2.12).



Діаграма 2.12 – Можливість повного переходу до електронного документообігу.

У кожного опитуваного своя відповідь, і, навіть, кілька аргументів чому, позитивного та негативного характеру, опис зовнішніх чинників впливу, ситуаціями, тощо.

Попри перевагу фахівців віком від 40 до 50 років, працівники використовують цифрові технології майже в усіх спектрах своєї повсякденної роботи: використання електронного суду юристами, робота у СЕД АСКОД кожного працівника та використання власного цифрового підпису при візуванні документів, доступне та повне функціонування сайту Комітету та суб-сайту Відділення, де кожен зможе швидко знайти усю необхідну інформацію, використання платформ та інших інформаційних систем для пошуку інформації у справах, особливо робота з офіційними майданчиками тендерних закупівель (саме ці системи демонструють відкритість та прозорість проведення торгів), чисельні навчання через онлайн ресурси, як, до прикладу, «Дія. Цифрова освіта», та інше.

Відповідно до цього можна стверджувати про відповідність державних службовців до вимог цифрового суспільства.

РОЗДІЛ 3. ТРАНСФОРМАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ ДО ВИМОГ ЦИФРОВОГО СУСПІЛЬСТВА.

3.1 Зміни в стратегії трансформації публічного управління в умовах цифрового суспільства.

Задля наближення публічного управління у відповідність вимог цифрового суспільства необхідне виокремлення напрямків реалізації цієї ідеї.

Так як суспільство є більш наближеним до цифрового світу, державні органи повинні швидко та якісно адаптуватись та вміло використовувати сучасні цифрові технології.

До стратегічних напрямів трансформації публічного управління до вимог цифрового суспільства варто віднести:

1. Уніфікація публічного управління.

Уніфікація державного управління – це ефективна можливість збільшення рівня прозорості управлінської діяльності. Саме процес уніфікації у багатьох уряд світу став запорукою наближення процесів надання різного виду послуг більш якісним та повним, за допомогою стандартизації структур, їх діяльності та функцій. Створення єдиної онлайн системи органів державної влади допоможе громадянам та державі уникнути бюрократизму, економити час та фінанси, швидко шукати перевірену та актуальну інформацію та використовувати максимум можливостей з отримання та надання адміністративних послуг.

На сьогодні, в Україні функціонує уніфікований портал органів державної влади – «Єдиний веб-портал органів виконавчої влади України». У ньому зібрані усі державні сайти України.

Проте варто зауважити, що внесення актуальної інформації є запорукою належної роботи відповідної структури. Більшість органів публічного управління нехтують стандартами що ускладнює процес та викликає недовіру збоку користувачів. Проаналізувавши сайт Антимонопольного комітету України варто зазначити, що актуалізація новин,

доопрацювання розділів, тем та сторінок відбулась лише в у жовтні місяці 2022 року.

2. Створення та забезпечення «цифрового» робочого місця.

«Цифрове» робоче місце є важливим та необхідним аспектом підвищення продуктивності, мобільності та ефективності роботи працівника. Створення належних умов праці у вигляді технічного забезпечення, постійного виходу до мережі Інтернет та динамічності роботи створює злагоджений колектив, підвищує рівень комунікацій, дозволяє працівникам швидко та якісно виконувати покладені обов’язки у короткі терміни та залученням мінімального напруження.

До прикладу, Антимонопольний комітет України забезпечує працівника робочим місцем укомплектованим комп’ютером, постійним доступом до мережі Інтернет через пряме підключення або через WiFi, принтерами та сканерами, доступом до великої кількості реєстрів відповідно до посадових обов’язків, тощо.

3. Доступна інформація для суспільного сектору або «Відкиті дані»

Доступ до відкритої інформації є першочерговим проявом забезпеченням прозорості та відкритості влади для громадськості. Відповідно до ст. 3 Закону України «Про доступ до публічної інформації» - право на доступ до публічної інформації гарантується:

1) обов'язком розпорядників інформації надавати та оприлюднювати інформацію, крім випадків, передбачених законом;

2) визначенням розпорядником інформації спеціальних структурних підрозділів або посадових осіб, які організовують у встановленому порядку доступ до публічної інформації, якою він володіє;

3) максимальним спрощенням процедури подання запиту та отримання інформації;

4) доступом до засідань колегіальних суб'єктів владних повноважень, крім випадків, передбачених законодавством;

5) здійсненням парламентського, громадського та державного контролю за дотриманням прав на доступ до публічної інформації;

6) юридичною відповідальністю за порушення законодавства про доступ до публічної інформації.

Доступ до інформації у вигляді публікування та надання відкритих даних є інструментом контролю держави громадянами, та, у кінцевому результаті, відкриті дані підвищують рівень довіри суспільства до органів влади.

Для забезпечення цього стратегічного кроку було створено «Портал відкритих даних» для загального користування громадянами, органами влади, організаціями, підприємствами, структурами, засобами масової інформаціями, тощо. Цей портал не є єдиним носієм відкритої інформації, проте, варто зауважити, що до такої інформації не відносяться до торгових марок чи авторських прав.

4. Залучення громадян до прийняття управлінських рішень.

Залучення громадян до управлінської діяльності є прямим слідуванням нормам Конституції України, а саме - громадяни мають право брати участь в управлінні державними справами, у всеукраїнському та місцевих референдумах, вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування.

Зменшення дистанції держави з громадянином є запорукою створення демократичної держави. Засобами такого виду комунікації є використання сайтів, опитувань, соціальних мереж, реалізація впровадження, належного розгляду та надання відповідей на е-петиції та проведення е-консультацій.

5. Електронна ідентифікація громадян.

При існуванні загрози кібернебезпек та шахрайства шляхом підробки документів є необхідність підвищення надійності цифрової ідентифікації особи.

Електронна ідентифікація громадянина допомагає створити громадянину безпечний простір для отримання необхідних послуг чи інформації. Проте такий вид ідентифікації є необхідним та більш зручним та

швидшим, оскільки стандартний метод перевірки особисто є застарілим, доволі довгим та з великим відсотком підробки та недостовірності.

На державному рівні вже впроваджена інтегрована система електронної ідентифікації, що об’єднала всіх надавачів послуг електронної ідентифікації: електронний підпис, BankID, MobileID.

6. Блокчейн.

Блокчейн – це база даних, що є розподіленою, ієрархічною та має вигляд ланцюгу. Основною ідеєю такої системи є те, що відповідно до посадових обов’язків та функцій особа може використовувати лише конкретні частини системи та опрацьовувати лише необхідні документи. Така система допомагає уникнути дублювань інформації, швидкій реєстрації та опрацюванню документу. В державному управлінні система блокчеїн використовується при опрацюванні е-звернень, е-петицій, е-референдумів та е-голосувань з надзвичайно високим рівнем захисту інформації.

7. Всебічна аналітика.

Аналітика, яка включає в себе збір та обробку інформації, допомагає державі розуміти правильність впровадження різного виду змін, актуальність та структурованість дій, роботи висновки задля поліпшення будь-якого спектру діяльності.

Всебічність аналітики надає можливість оцінки позитивності прийняття рішень. Аналітика відбувається на основі повної, актуальної, правдивої, відкритої, прозорої інформації задля поліпшення створення комунікаційних зв’язків держави та громадянина, підвищення рівня довіри та постійний прогрес та удосконалення державної влади.

Проведення референдумів, соціальних опитувань, журналістських розслідувань є процесами збору аналітичної інформації та засобами реалізації аналітичних процесів задля покращення управлінської діяльності.

Відповідно до вищезазначеної інформації можливо підтвердити відповідність держави до вимог цифрового суспільства.

3.2 Кібербезпека як основа взаємодії органів публічного управління з громадян у аспекті захисту інформації.

Реалії сьогодення свідчать про те, що кіберзагрози еволюціонують в прискореному темпі, кіберзлочини стають досконалішими, краще організованими і транснаціональними.

Це зумовлено тим, що інтернет, цифрові послуги, інформаційно-комунікаційні технології стали невід'ємною частиною економіки в усьому світі: від електронного документообігу, інтернет-магазинів та онлайнбанкінгу до систем інтернету речей та інтелектуальних систем управління підприємствами.

Зі зростанням залежності від використання цифрових технологій у бізнесі і підприємництві відповідно зростають кіберризики і кіберзагрози, що потребує завчасного реагування щодо їх запобігання або вирішення та обізнаності з факторами ризику всіх зацікавлених сторін.

Система кібербезпеки має працювати в інтересах громадськості як для постачальників послуг, так і для користувачів послуг. Саме держава як гарант прав і свобод громадян має взяти на себе відповідальність за забезпечення доступу до стабільного безпечного цифрового простору, яким можуть скористатися всі громадяни, адже забезпечення належного рівня кібербезпеки є необхідною умовою розвитку інформаційного суспільства.

Останнім часом суспільство дедалі частіше стикається з різноманітними видами кібератак: збої при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та конфіденційності даних, інформаційнопсихологічний тиск на населення, кібертероризм, кібершпигунство, інформаційна експансія у національний інформаційний простір країни, блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення й об'єктів підвищеної небезпеки.

Безумовно, першочергове поняття, яке необхідно розшифрувати є поняття кіберпростір, як зону дії кібербезпеки. [47]

Кіберпростір називають одним найбільшим нерегульованих і неконтрольованих доменів в історії людства, який також є унікальним, оскільки він є штучним доменом, створеним людьми з дуже короткою історією.

Кіберпростір є чіткою, широко поширеною, взаємопов'язаною цифровою технологією. Цей термін увійшов до популярної культури з наукової фантастики та мистецтва, але тепер використовується технологічними стратегами, фахівцями з безпеки, урядовими, військовими та промисловими лідерами та підприємцями для опису сфери глобального технологічного середовища.

Хоча деякі вчені вважають, що кіберпростір - це просто умовне середовище, в якому відбувається зв'язок через комп'ютерні мережі. Так наразі визначає кіберпростір Оксфордський словник [48].

На даний момент не існує спільних визначень кіберпростору на науковому рівні, і кожен уряд використовує окреме визначення.

Деякі країни, такі як Канада, називають кіберпростір "глобальними общинами", інші, як Німеччина, обмежують визначення всесвіту Інтернету, явно виключаючи інші типи мереж між комп'ютерами.

Локанічним є визначення кіберпростору, яке використовується в Пентагоні, а саме кіберпростір є національним середовищем, в якому оцифрована інформація передається через комп'ютерні мережі

Проте, найбільш поширене визначена слідує, що кіберпростір визначається як загальна система взаємопов'язаних комп'ютерних інфраструктур, включаючи апаратні засоби, програмне забезпечення, дані та користувачів, а також логічні зв'язки між ними, незалежно від того, як вони створені.

Кібербезпека існує лише у кіберпросторі, несучи за собою захист даних користувачів.

Президент України Володимир Зеленський своїм Указом № 447/2021 від 26 серпня 2021 року затвердив рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [50].

Стратегія кібербезпеки України, на сьогодні, визначає пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

У цій Стратегії визначено, що «забезпечення кібербезпеки є одним з пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі».

Наголошується, що «кіберпростір разом з іншими фізичними просторами визнано одним з можливих «театрів» воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі».

Відповідно до новоприйнятих нормативно-правових актів, все більшої небезпеки у вигляді взлому ваб-сайтів державних органів та інші заходи, щодо заволодіння інформацією або ж її обмеження прогнозує зростання інтенсивності міждержавного протиборства й розвідувально-підривної діяльності у кіберпросторі.

У Стратегії визначені основні виклики та загрози для України у сфері кібербезпеки, якими є:

- активне використання кіберзасобів у міжнародній конкуренції;
- змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій,

зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо;

- мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;
- вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;
- упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

Також варто підкреслити окрім основних суб'єктів національної системи кібербезпеки, Україна залучає до розв'язання завдань у цій сфері більш широке коло учасників, у тому числі суб'єктів господарювання, громадські об'єднання та окремих громадян України.

До пріоритетів забезпечення кібербезпеки України відносять:

- забезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;
- захист прав, свобод і законних інтересів громадян України у кіберпросторі;
- європейська і євроатлантична інтеграція у сфері кібербезпеки.

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації цієї Стратегії.

Для формування потенціалу стримування необхідним є досягнення таких стратегічних цілей (таб. 3.2):

Ціль 1	Дієва кібероборона;
Ціль 2	Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму;
Ціль 3	Ефективна протидія кіберзлочинності;
Ціль 4	Розвиток асиметричних інструментів стримування.

Таб. 3.2.2 – Цілі Стратегії формування національної системи кібербезпеки.

Для набуття кіберстійкості необхідним є досягнення таких стратегічних цілей (таб. 3.3):

Ціль 1	Національна кіберготовність та надійний кіберзахист;
Ціль 2	Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки;
Ціль 3	Безпечні цифрові послуги.

Таб. 3.3 - Цілі набуття кяіберстійкості.

Чи готове суспільство до вимог кібербезпеки? Задаючи таке питання шокує скільки інформації є відкритому доступі щодо курсів з кібербезпеки чи кібергігієни.

Проте, мало хто розуміє і знає звідки можливо чекати небезпеку. Тому необхідно більш детально дослідити поняття «кіберзагрози» та «кіберризику».

Кібернетичні загрози (кіберзагрози) - існуючі та потенційно небезпечні загрози інтересам людей, суспільств і націй через порушення доступності, цілісності та достовірності режимів доступу до інформації.

Можливі явища та фактори, що циркулюють у важливих об'єктах інформаційна інфраструктура країни.

Зауважте, що загрози – це не факти чи події. У будь-якому випадку це дія.

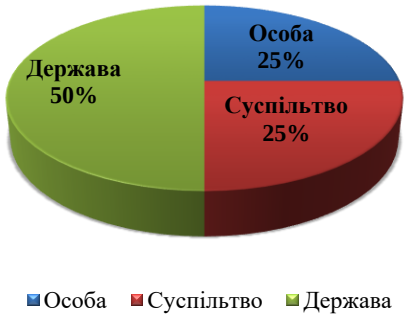
Поняття «кіберзагроза» – це протиправна та карана дія суб’єкта інформаційних правовідносин, що створює небезпеку для життєво важливих інтересів особи, суспільства та держави в цілому, від вчинення якої залежить належне функціонування. інформаційні, телекомунікаційні та інформаційні

системи, а також відносини щодо створення, збору, отримання, зберігання, використання, поширення, захисту та захисту інформації.

Базуючись на даному визначенні, зауважу, що зміст, тобто сутність кіберзагроз становлять їх суб'єкти, тобто суб'єкти інформаційних правовідносин, а об'єктом є безпосередньо інформація.

У Доктрині інформаційної безпеки України, що втратила чинність, було зазначено, що в інформаційній сфері України вирізняються такі життєво важливі інтереси (діаграма 3.1):

Діаграма 3.1 - Сфери захисту у кіберпросторі



1) особа: належне забезпечення конституційних прав та свобод особи на збір, зберігання, використання та поширення інформації. Запобігання несанкціонованому втручанню в процес змісту, обробки, передачі та використання персональних даних, захист від негативного інформаційно-психологічного впливу;

2) суспільство: збереження та примноження духовних, культурних і моральних цінностей українського народу. Забезпечення соціально-політичної стабільності, злагоди між етносами та професіями. Становлення та розвиток демократичних інститутів громадянського суспільства;

3) держава: запобігання інформаційній залежності, інформаційній блокаді в Україні, інформаційній експансії з боку інших країн та міжнародних організацій. Ефективна взаємодія національних органів влади та інститутів громадянського суспільства у формуванні, реалізації та координації національної політики в інформаційній сфері. Побудова та

розвиток інформаційного суспільства. забезпечення економічного, науково-технічного розвитку України; формування позитивного іміджу України інтеграція України у світовий інформаційний простір.

Кіберзагроза – вид загрози, реалізація якої пов'язана з використанням суміжних ресурсів інформаційно-комунікаційних систем. Уразливими до реалізації кіберзагроз є об'єкти, функції комп'ютерної системи яких пов'язані з використанням ресурсів кіберпростору. Іншими словами, об'єкти, які можуть постраждати від кібератак, безпосередньо залежать від онлайн-мереж. До об'єктів національної критичної інфраструктури, що потребують захисту від кібератак, необхідно віднести такі види наслідків загроз як:

- надзвичайна ситуація;
- блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств,
- систем життєзабезпечення та об'єктів підвищеної небезпеки; блокування роботи державних органів;
- блокування діяльності органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю;
- порушення безпечного функціонування банківської або фінансової системи держави;
- розголошення державної таємниці;
- масові заворушення.

Тобто, кіберзагрози не можна обмежувати якоюсь однією сферою і, частіше за все, настання певних наслідків може спричинити інші, більш глобальні.

Неналежне правове регулювання в національному кібернетичному просторі України провокує низьку негативних явищ, які створюють реальні та потенційні загрози кібернетичній безпеці. Як приклад, у 2014 році на території Автономної Республіки Крим та південно-східних регіонах України

здійснювався інформаційно-психологічний тиск на населення України з боку засобів масової інформації РФ, спостерігалася інформаційне втручання та захоплення національного інформаційного простору України, захоплювались стратегічні об’єкти української телекомунікаційної інфраструктури.

Розвиваючи далі ідею загроз у сфері кібербезпеки, зауважу, що існує залежність країни і в інформаційному, і смисловому вимірах. Це коли країні не вистачає власних новин чи власних фільмів, і вона заповнює ці прогалини чужим продуктом. Україна є чітким прикладом цієї ситуації. Так само можу зазначити, що і Європа виявилася нездатною протистояти навалі інформаційного бруду з Росії, сформувати ефективну систему інформаційної політики, включаючи механізми нейтралізації дезінформаційних потоків з Росії.

Інформаційне втручання становить значну загрозу кібербезпеці, оскільки кібербезпека є частиною національної безпеки і може завдати шкоди як цілим націям, так і окремим особам. Для створення ефективної системи забезпечення кібербезпеки українські державні інституції мають чітко визначити правові основи національної політики у цій сфері та розуміти динамічні зміни, які відбуваються у світі у сфері кібербезпеки, мають своєчасно реагувати. Можливість застосування міжнародного досвіду.

При цьому, вибір конкретних засобів і способів забезпечення кібернетичної безпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кібернетичних загроз життєво важливим інтересам людини і громадянина, суспільства і держави.

На сьогодні, виокремлюють такі загрози кібербезпеці і безпеці інформаційних ресурсів:

- уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;
- фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Україна має швидко, надійно та ефективно реагувати на будь-які кіберзагрози, що неможливо без інтегрування та чіткої взаємодії всіх наявних ресурсів суб'єктів кібербезпеки.

Аналіз законодавства у сфері кібербезпеки, а також організаційних заходів, спрямованих на розбудову ефективних систем кіберзахисту провідних країн світу свідчить, що ключові світові гравці вдосконалюють власні можливості з кіберзахисту відповідно до трансформації сучасних кіберзагроз.

Останнім часом фіксується суттєва зміна форм, суб'єктів і наслідків реалізації основних загроз кібербезпеці держав. Так, кібератаки стають все більш комплексними та складними, їх наслідки становлять загрозу ключовим національним інтересам, а їхніми організаторами або замовниками все частіше виявляються спецслужби іноземних держав чи терористичні організації.

Потреба реалізації ефективних заходів із протидії сучасним кібернетичним загрозам на національному рівні приводить до збільшення ролі в системах кібербезпеки країн спеціальних служб та правоохоронних органів, що мають контррозвідувальні функції і виконують завдання із протидії протиправній діяльності спецслужб іноземних держав та тероризму.

В Україні розпочато створення Центру оперативного реагування на загрози у сфері кібернетичної безпеки, допомогу якому надає уряд США. Здійснюються заходи щодо впровадження в діяльність Міноборони та ЗСУ засобів із захисту інформації в інформаційно-телекомунікаційних системах з урахуванням стандартів провідних країн світу. Також розроблено проект Стратегії кібероборони України, який вже погоджений з представниками європейського командування Збройних сил США, Агенції з національної безпеки Чеської Республіки. Наразі цей документ знаходиться на розгляді профільного комітету Верховної Ради та апарату РНБО.

Національний банк України та Незалежна асоціація банків України планують створити спільний центр реагування альянсу в банківській системі.

Керівництвом НБУ презентовано проект створення «Центру реагування на інциденти кібернетичної безпеки у банківській системі та платіжному просторі України CERT-NBU». Відповідно до своєї головної мети створення CERT-NBU повинно допомогти у вирішенні проблем боротьби з кіберзагрозами і буде сприяти розвитку банківської системи України в цілому.

Також варто акцентувати увагу на тому тому, що кібербезпека не може регулюватися лише на національному або європейському рівні, для цього необхідні глобальні зв'язки.

У питаннях протидії кіберзагрозам повинні застосовуватися принципово нові механізми. Ефективним засобом протидії кіберзагрозам може стати розбудова нових ліній оборони, однією з яких має стати міжнародне співробітництво між всіма зацікавленими акторами. З тим, щоб у разі кібератаки компетентні органи сторони, яка зазнала нападу, і сторони, з території якої походить кібератака, оперували механізмами оперативного сповіщення про такий інцидент, а також спільної боротьби з ним.

Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективно діючу систему протидії загрозам в кіберпросторі.

До таких проблем в першу чергу відносяться: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим наповненням відповідних структурних підрозділів, обізнаність населення та службовців.

Проте, Україна швидко навчається і допомагає громадянам опанувати основні закони та правила кібергігієни.

ВИСНОВКИ

Ідея створення «цифрової держави» є надзвичайно складним, але необхідним кроком для України. Беручи до уваги тісну взаємодію держави із громадськістю, впровадження цифрових технологій у діяльність державної влади є потужним кроком до реалізації цієї ідеї.

Цифровізація поступово проникає майже в усі аспекти життя як громадян, так і державних службовців.

Варто зазначити про основні нормативно-правові акти, що регуюлюють сферу діяльності органів публічного управління в умовах цифрового суспільства:

- Конституція України
- Міжнародна хартія відкритих даних;
- Закон України «Про електронні довірчі послуги»;
- Закон України «Про доступ до публічної інформації»;
- Закон України «Про звернення громадян»;
- Порядок розгляду електронної петиції, адресованої Президентові України;
- Порядок розгляду електронної петиції, адресованої Кабінету Міністрів України;
- Розпорядження Голови Верховної Ради України щодо забезпечення документообігу у Верховній Раді України в електронній та паперовій формах;
- Закон України «Про електронні документи та електронний документообіг»;
- Закон України «Про Національну програму інформатизації»;
- Закон України «Про Національну систему конфіденційного зв'язку»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

- Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації

Зважаючи на те, що цифровізація охоплює як політичну, та і соціальну сфери можливо зробити такі висновки.

У політичній сфері оцифровування відображається в трансформації внутрішніх і зовнішніх відносин на основі використання інформаційних технологій та оптимізації роботи державних адміністрацій.

Основними позитивними показниками впровадження цифровізації є відкритість та прозорість діяльності агентства. Це робить державні установи більш гнучкими, менш ієрархічними та менш регульованими.

Підвищення рівня залученості громадян до аналізу та прийняття державних рішень сприяє максимізації ефективності та ефективності державного управління, що свідчить про те, що демократії сповна розкривають свою славу.

Зокрема, впровадження електронного урядування використовує інформаційні технології для трансформації контролю. Залучення громадян здійснюється шляхом створення електронних петицій, електронних звернень та електронних консультацій.

Також організація інформаційної взаємодії між органами державної влади всіх рівнів дає змогу створити централізовану (загальну) базу даних. Впроваджуючи повноцінний електронний документообіг з використанням електронного цифрового підпису, створюється єдина інформаційно-аналітичну система діяльності органів державної влади та місцевого самоврядування.

Якщо говорити про соціальний сектор, то зазначимо, що основним завданням є підвищення рівня задоволеності громадян державними послугами. Це значно розширить можливості самообслуговування громадян, прискорить і спростить проходження адміністративних процедур, усуне дублювання різних завдань, розширить можливості для навчання

(дистанційної освіти), сприятиме зростанню громадян. Цифрова та технологічна обізнаність і, найголовніше, підвищення рівня довіри до влади.

Проте, існують фактори стримування втілення поставлених задумів:

1. цифрова нерівність (не всі громадяни мають рівні можливості доступу до Інтернету через технологічні чи географічні проблеми, або через недостатнє матеріальне забезпечення чи фізичні вади),
2. рівень освіти та навичок громадян та державних службовців,
3. проблеми конфіденційності у аспекті захисту інформації,
4. тощо.

Основним питанням мого дослідження є напрями трансформації публічного управління в умовах цифрового суспільства. Під цими напрямами розуміються засоби та способи впровадження цифровізації у органах державної влади.

Не рідко, громадяни є більш обізнаними у сфері користування інформаційними системами, і основною сферою реалізації цього факту став бізнес, який тісно пов'язаний із міжнародним ринком та цифровими технологіями.

Саме тому, надзвичайно актуальною темою є готовність державної служби до вимог цифрового суспільства.

Основним напрямком роботи став аналіз теперішньої ситуації впровадження цифрових технологій на рівні держави.

Розвиток телекомунікаційних систем і мереж в малих містах і селах, підвищення рівня комп’ютерної грамотності серед населення, впровадження різного роду заохочень та проведення загальних просвітницьких кампаній з метою поступового ознайомлення громадян з цифровими технологіями є величезним вкладом до реалізації ідеї «цифрової держави».

Впровадження технології електронного урядування – це створення якісного та сучасного ринку інтелектуальних послуг, розвиток телекомунікаційної інфраструктури та успішна робота в конкурентному середовищі з використанням останніх досягнень науки і техніки. Однак

перешкоди, пов'язані з уніфікацією та стандартизацією технологій і структур даних, неможливо подолати без кваліфікованих і компетентних співробітників, які володіють навичками використання інформаційних систем. Органи влади та організації. Тому комунікація між різними органами влади та між суспільствами є важливою.

Держава зрозуміла, що неможливо інтегруватися в національний та світовий економічний простір, налагодити взаємодію та співробітництво з державними органами зарубіжних країн та міжнародними організаціями, не використовуючи технології електронного урядування.

Ватро підкреслити, що відповідно до проведеного опитування працівників державної служби у Південно-західному міжобласному територіальному відділені Антимонопольного комітету України можливо зробити такі висновки.

Працівники Відділення в повній мірі володіють цифровою компетентністю, що спостерігається в наступному.

Попри перевагу фахівців віком від 40 до 50 років, працівники використовують цифрові технології майже в усіх спектрах своєї повсякденної роботи: використання електронного суду юристами, робота у СЕД АСКОД кожного працівника та використання власного цифрового підпису при візуванні документів, доступне та повне функціонування сайту Комітету та суб-сайту Відділення, де кожен зможе швидко знайти усю необхідну інформацію, використання платформ та інших інформаційних систем для пошуку інформації у справах, особливо робота з офіційними майданчиками тендерних закупівель (саме ці системи демонструють відкритість та прозорість проведення торгів), чисельні навчання через онлайн ресурси, як, до прикладу, «Дія. Цифрова освіта», та інше.

Важливим елементом впровадження цифровізації є повна та всебічна безпека та захист інформації. Із введенням воєнного стану через військову агресію РФ, держава зрозуміла надзвичайну важливість та колосальну необхідність у якісному кіберзахисті.

Кібергнебезпека з початку повномасштабного вторгнення РФ на територію України зазнала піку та посіяла паніку серед органів державної влади, органів місцевого самоврядування та звичайних користувачів інформаційних мереж. Вміння захищати власну інформацію від зловмисників, користуватися перевіреними джерелами інформації та фільтрувати інформацію є важливим внеском кожного у цифрову безпеку держави у кіберпросторі.

Кожен крок до повного впровадження цифровізації у державній службі наближує владу до суспільства.

Цифрове суспільство розвивається та поширюється швидше ніж електронне врядування. Саме тому, держава повинна заохочувати працівників до підвищення власної цифрової компетентності за допомогою не лише онлайн навчань через загальні платформи, а й беручи досвід інших передових країн-партнерів світу.

Україна досить молода та прогресивна країна, проте залишки радянського союзу нівелюють та сповільнюють створення нової цифрової та демократичної держави.

Саме тому перспективи такого стрімкого створення «держави у смартфоні» допоможе нарешті об’єднати такі далекі категорії як влада та суспільство, шляхом повної довіри громадян до держави на основі відкритості, прозорості та доступності влади для кожного.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бойко Н. Інтернет як ресурс демократизації українського суспільства : Автореферат. Київ, 2021. 30 с.

2. Духовна О. Україна «в цифрі». *Юридична онлайн газета*. 2019. 5 листоп. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ukrayina-v-cifri-napryamki-reformuvannya.html.

3. Бурдін М. Ю. Особливості формування «електронної держави» // Харківський національнийуніверситет внутрішніх справ: 20 років у статусі національного : матеріали Міжнар. наук.-практ.конф. (м. Харків, 2 берез. 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2021.

4. Мукомела І. В. Правові засади інформаційного суспільства: загальнотеоретичний аналіз: автореферат дисертації. канд. юрид. наук : Харків, 2016. 23 с.

5. Поченчук Г. Теоретичні аспекти інституціонального реформування. *Науковий вісник.*

6. Данилов А. Д., Соловйова К. О. Напрями державної інформаційної політики України : Thesis. 2016. URL: http://openarchive.nure.ua/handle/document/6114

7. Турченко Ю. В. Реалізація державної інформаційної політики України у сфері оборони : дис. … канд. політ. наук. Київ, 2013. 200 с.

8. Ю. Л. Мохова, А. І. Луцька. Сутність та головні напрямки державної інформаційної політики України : дис. … канд. наук з держ. упр. м. Покровськ, 2018. 7 с. URL: https://doi.org/10.32702/2307-2156-2018.12.25.

9. Збожинський С. Інформаційна безпека під час застосування цифрових технологій. *Юридична газета*. 2017. 17 жовт. С. 18–19.

10. Матвієнко О. Цифровізація : освітній контекст. *Вісник Книжкової палати*. 2020. № 11 (292), листоп. С. 28–35.

11. Мурач Д., Теліженко Л. Соціальні мережі в особистому та професійному житті працівників державної служби. *Modalităţi conceptuale de dezvoltare a ştiinţei moderne*. 2020. URL: https://doi.org/10.36074/20.11.2020.v4.27

12. Татарінцева А. В. Кібербезпека як складова частина національної безпеки україни : Thesis. 2018. URL: http://er.nau.edu.ua/handle/NAU/32748

13. Степанов В. Ю. Цифрова дипломатія як інструмент масової комунікації в публічному управлінні. *Вісник Національної академії державного управління при Президентові України. Серія "Державне управління"*. 2020. № 3 (98). С. 5–10.

14. Оболенський О. Опорний конспект лекцій в навчальної дисципліни «Публічне управління»: наук, розробка. К.: НАДУ. 2011. 56 с.

15. Український інститут майбутнього. *Економічна стратегія України 2030 >> Український інститут майбутнього*.

16. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : Розпорядж. Каб. Міністрів України від 17.01.2018 р. № 67-р : станом на 17 верес. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-р#Text

17. Пірен М. Бюрократизм у системі діяльності політико-владної еліти україни як чинник конфліктності влади і народу. *Актуальні проблеми навчання та виховання людей з особливими потребами*. 2007. URL: http://ap.uu.edu.ua/article/259.

18. 2021 corruption perceptions index - explore the results. *Transparency.org*. URL: https://www.transparency.org/en/cpi/2021

19. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII : станом на 1 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

20. Система "Трембіта". URL: https://dir.gov.ua/projects/trembita

21. Деякі питання приєднання до Міжнародної хартії відкритих даних : Розпорядж. Каб. Міністрів України від 22.09.2016 р. № 686-р : станом на 25 лют. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/686-2016-р#Text

22. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI : станом на 19 лют. 2022 р.
URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

23. Дія.Відкриті дані. *Дія.Відкриті дані*. URL: https://diia.data.gov.ua/

24. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

25. Про звернення громадян : Закон України від 02.10.1996 р. № 393/96-ВР : станом на 1 січ. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/393/96-вр#Text

26. Про Порядок розгляду електронної петиції, адресованої Президентові України : Указ Президента України від 28.08.2015 р. № 523/2015. URL: https://zakon.rada.gov.ua/laws/show/523/2015#Text

27. Про затвердження Порядку розгляду електронної петиції, адресованої Кабінету Міністрів України : Постанова Каб. Міністрів України від 22.07.2016 р. № 457 : станом на 7 листоп. 2018 р. URL: https://zakon.rada.gov.ua/laws/show/457-2016-п#Text

28. Про деякі питання забезпечення документообігу у Верховній Раді України в електронній та паперовій формах (Положення про порядок роботи з документами у Верховній Раді України) : Розпорядж. Голови Верхов. Ради України від 08.02.2021 р. № 19 : станом на 28 жовт. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/19/21-рг#Text.

29. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV : станом на 1 серп. 2022 р.
URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

30. Модельний закон про інформатизацію, інформацію та захист інформації : Модель Співдружності незалеж. держав від 18.11.2005 р.
URL: https://zakon.rada.gov.ua/laws/show/997_d09#Text

31. Про Національну програму інформатизації : Закон України від 04.02.1998 р. № 74/98-ВР : станом на 1 січ. 2022 р.
URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text

32. Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV : станом на 1 січ. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text

33. Про Національну систему конфіденційного зв'язку : Закон України від 10.01.2002 р. № 2919-III : станом на 1 січ. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2919-14#Text

34. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 1 лип. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

35. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 р. № 1229/99 : станом на 4 трав. 2008 р. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text

36. Деякі питання цифрової трансформації : Розпорядж. Каб. Міністрів України від 17.02.2021 р. № 365-р : станом на 15 верес. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/365-2021-р#Text

37. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації : Розпорядж. Каб. Міністрів України від 17.11.2021 р. № 1467-р. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-р#Text

38. Дія. Цифрова Освіта. *Дія. Цифрова Освіта*. URL: https://osvita.diia.gov.ua/

40. Портал відкритих даних. *Головна сторінка - Data.gov.ua*. URL: https://data.gov.ua/

41. Prozorro. *Головна | Prozorro*. URL: https://prozorro.gov.ua/

42. Державні публічні закупівлі в Україні: тендери, аукціони, закупки, торги | Веб портал державних закупівель Prozorro. *Державні публічні закупівлі в Україні: тендери, аукціони, закупки, торги Веб портал державних закупівель Prozorro*.
URL: https://www.dzo.com.ua/?utm_source=google&utm_medium=cpc&utm_campaign=prozorro&utm_content=prozorro&utm_term=прозоро&gclid=CjwKCAiAdCcBhBQEiwAeWidtc9t_8W86zrWnv6lP4rFbjBBa51HjQvG_6czvQrXYHhUrDTnxwkjBoCdcUQAvD_BwE

43. E-Тендер. URL: https://e-tender.ua/ru/prozorroprodagy?gclid=CjwKCAiAdCcBhBQEiwAeWidtSR8XBJrac1opg0iNk2MAlyxohPI7V2ilTyrj7ut8CP1PV8NV7iAjRoCe4QQAvD_BwE

44. SmartTender – відкриті тендери в Україні, державні та комерційні закупівлі Prozorro. *SmartTender – відкриті тендери в Україні, державні та комерційні закупівлі Prozorro*.
URL: https://smarttender.biz/?utm_medium=cpc&utm_source=google&utm_campaign=Prozorro_Brand_EXP&utm_term=prozorro&gclid=CjwKCAiAdCcBhBQEiwAeWidtTu7ieTspCQqe7O70f6E_FootWu-I7FawM0Ji_OgWV-cuDxvHkETaxoCGuAQAvD_BwE

45. 2021 Corruption Perceptions Index - Explore the results. *Transparency.org*. URL: https://www.transparency.org/en/cpi/2021

46. Міністерство цифрової трансформації України. *Єдиний веб-портал органів виконавчої влади*. URL: https://www.kmu.gov.ua/catalog/ministerstvo-cifrovoyi-transformaciyi.

47 Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : дис. … канд. політ. наук. Київ, 2014. 318 с. URL: https://shron1.chtyvo.org.ua/Dubov_Dmytro/Kiberprostir_iak_novyi_vymir_heopolitychnoho_supernytstva.pdf?PHPSESSID=v6qi07pngjopfgqhltohmhtrd2.

48. Оксфордський словник англійської мови. «Oxford University Press».

49. Електронна петиція. *Довідник громадського активіста*. URL: http://dovidnyk.org.ua/informatsiina-prozorist-3/elektroni-petytsii.

50. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

51. Міністерство соціальної політики України. Костянтин Кошеленко про результтати цифровізації соціальної сфери, 24.11.2022. *Facebook*. URL: https://fb.watch/hoK8MnnLaq/.

52. Антимонопольний комітет україни - головна. *Головна | Антимонопольний комітет України*. URL: https://amcu.gov.ua/

53. Про вимоги до форматів даних електронного документообігу в органах державної влади. Формат електронного повідомлення : Наказ МОН, молоді та спорту України від 20.10.2011 р. № 1207. URL: https://zakon.rada.gov.ua/laws/show/z1306-11#Text

54. Про делегацію України для участі у переговорах з Європейською Комісією щодо укладення Угоди між Україною та Європейським Союзом про участь України в програмі Європейського Союзу "Цифрова Європа" (2021 - 2027) : Розпорядж. Президента України від 19.07.2022 р. № 133/2022-рп. URL: https://zakon.rada.gov.ua/laws/show/133/2022-рп#Text

55. Про затвердження Переліку і Порядку надання інформаційних та інших послуг з використанням електронної інформаційної системи "Електронний Уряд" : Наказ Держ. ком. зв'язку та інформатизації України від 15.08.2003 р. № 149 : станом на 26 верес. 2004 р. URL: https://zakon.rada.gov.ua/laws/show/z1065-03#Text

56. Про затвердження Положення про Веб-сайт Верховної Ради України у глобальній інформаційній мережі Інтернет : Розпорядж. Голови Верхов. Ради України від 24.05.2001 р. № 462 : станом на 19 трав. 2015 р. URL: https://zakon.rada.gov.ua/laws/show/462/01-рг#Text

57. Про затвердження Положення про Центральний державний електронний архів України : Наказ М-ва юстиції України від 21.05.2012 р. № 759/5. URL: https://zakon.rada.gov.ua/laws/show/v0759323-12#Text

58. Про затвердження Порядку загальнодержавного топографічного і тематичного картографування : Постанова Каб. Міністрів України від 04.09.2013 р. № 661 : станом на 2 груд. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/661-2013-п#Text

59. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади : Постанова Каб. Міністрів України від 04.01.2002 р. № 3 : станом на 25 верес. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/3-2002-п#Text

Виконала:
студентка магістратури
за спеціальністю 281 Публічне
управління та адміністрування
заочної форми навчання

_____ _____

Дар'я
ЯКИМЧУК

Науковий керівник:
доцентка кафедри публічного
управління та адміністрування,
к. держ. упр., доцентка

_____ _____

Людмила
ТРЕБИК

Робота допущена до захисту:
завідувач кафедри публічного
управління та адміністрування,
д. держ.упр., доцент

_____ _____

Едуард
ЩЕПАНСЬКИЙ