

**Міністерство освіти і науки України  
Державний торговельно-економічний університет  
Вінницький торговельно-економічний інститут  
Кафедра менеджменту та адміністрування**

## **КВАЛІФІКАЦІЙНА РОБОТА**

на тему:

**«Системи цифрової ідентифікації в публічному  
управлінні» (за матеріалами Міністерства цифрової  
трансформації, м. Київ)**

Здобувача вищої освіти  
II курсу, групи ПУА-21з(м),  
спеціальності 281 «Публічне управління  
та адміністрування»  
освітньої програми «Публічне управління  
та адміністрування»  
заочної форми навчання

Богдани  
Баяк

Науковий керівник  
канд. екон. наук

Ірина  
Семенюк

Гарант освітньої програми  
канд. наук держ. упр., доцент

Ірина  
Ніколіна

Вінниця 2023

## ЗМІСТ

|                                                                                                                         |    |
|-------------------------------------------------------------------------------------------------------------------------|----|
| ВСТУП                                                                                                                   | 3  |
| РОЗДІЛ 1 КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА РОЛЬ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ У ПУБЛІЧНОМУ УПРАВЛІННІ                                    | 6  |
| РОЗДІЛ 2 АНАЛІЗ СУЧАСНОГО СТАНУ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ В УКРАЇНІ ТА ЇЇ ВПЛИВ НА РОЗВИТОК ПУБЛІЧНОГО УПРАВЛІННЯ          | 18 |
| 2.1 Правові засади діяльності та організаційно-функціональна характеристика Міністерства цифрової трансформації України | 18 |
| 2.2 Основні проблеми та виклики функціонування цифрової ідентифікації                                                   | 23 |
| РОЗДІЛ 3 ВИЗНАЧЕННЯ ПРІОРИТЕТНИХ НАПРЯМКІВ УДОСКОНАЛЕННЯ СИСТЕМИ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ В ПУБЛІЧНОМУ УПРАВЛІННІ.        | 37 |
| 3.1 Забезпечення захисту конфіденційності та безпеки як пріоритетний напрямок удосконалення цифрової ідентифікації      | 37 |
| 3.2 Забезпечення доступності, інтеграції та співпраці в контексті удосконалення цифрової ідентифікації                  | 43 |
| ВИСНОВКИ ТА ПРОПОЗИЦІЇ                                                                                                  | 54 |
| СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ                                                                                              | 56 |
| ДОДАТКИ                                                                                                                 |    |

## ВСТУП

*Актуальність теми.* У сучасному світі, де все більше частин нашого життя стає цифровими, електронна ідентифікація є важливим інструментом для захисту даних і зручного та ефективного спілкування між громадянами та владою. Вона вимагає розробки відповідних стратегій, технологічних рішень і законодавчої бази, щоб протистояти викликам, які виникають у сучасному світі.

У сфері публічного управління проблема цифрової ідентифікації є актуальною та має значення для багатьох аспектів сучасного суспільства та державного управління.

Ця тема стала предметом досліджень у багатьох наукових працях і публікаціях. Ось деякі вчені, що її досліджували: J. D. Lasica, David Yoon, Chunming Rong, Martin Gilje Jaatun, Paul M. Wagenseil, Дурман М. О., Дурман О. Л., Лінецька Я. М., Карпенко О. В., Карпенко Ю. В., Клименко А. В., Гбур З. В., Малий І. Й., Цедік М. Г., Мохова Ю. Л., Наместнік В. В., Новицький О. В., Копанєва О. В. [34], Костенко Л. Й. [30], Головобородько А. [25], Корчан В., Морозова І. [31] Краус, К. М., Краус, Н. М. [32] та інші.

*Гіпотеза дослідження* базується на припущенні, що цифрова ідентифікація має позитивний вплив на публічне управління шляхом полегшення доступу громадян до послуг та оптимізації адміністративних процедур. Таким чином, впровадження цифрової ідентифікації в публічному управлінні сприяє покращенню ефективності адміністративних процедур та забезпечує зручність для громадян.

*Мета дослідження.* Дослідити роль та вплив цифрової ідентифікації на публічне управління в сучасному інформаційному суспільстві з метою розкриття її переваг та викликів для ефективності адміністративних процедур, захисту приватності громадян і покращення якості публічних послуг.

*Завдання дослідження,* які впливають з його мети:



1. Розглянути теоретичні підходи до цифрової ідентифікації та визначити ключові концепції та технології, пов'язані з нею, для з'ясування її ролі в публічному управлінні.

2. Провести детальний аналіз впливу цифрової ідентифікації на ефективність адміністративних процедур та публічних послуг, враховуючи особливий акцент на Міністерстві цифрової трансформації України як об'єкті аналізу.

3. Розробити конкретні рекомендації для оптимізації використання цифрової ідентифікації в адміністративних процедурах та публічних послугах, враховуючи висновки з аналізу, і запропонувати практичні кроки та інструменти для впровадження рекомендацій у реальних умовах публічного управління.

*Об'єктом дослідження* є системи цифрової ідентифікації в публічному управлінні.

*Предмет дослідження* - процес впровадження та функціонування систем цифрової ідентифікації на рівні діяльності Міністерства цифрової трансформації України.

*Методи дослідження.* В роботі вивчений і розроблений матеріал викладено за допомогою системного підходу. Використовувалися такі методи, як логічне пізнання, синтез, порівняння, прогнозування та дедуктивна аргументація.

*Інформаційну базу дослідження* становлять Закон України «Про електронні довірчі послуги», Положення про Міністерство цифрової трансформації України; інші офіційні документи, звіти, законодавство та рішення, які стосуються цифрової ідентифікації та її регулювання в Україні; результати анкетування громадян у форматі Google-форм: дані, отримані в ході організації фокус-груп, офіційні сайти, науково-аналітичні статті зарубіжних та вітчизняних авторів, що стосуються теми, щоб забезпечити додатковий контекст та підтримку аргументів у роботі.

*Наукова новизна.* Подальшого розвитку набули теоретико-методологічні засади аналізу та розробки рекомендацій щодо взаємодії громадян з системами цифрової трансформації в контексті здійснення еволюційних змін в публічному управлінні.

*Практична цінність* даного дослідження виявляється у конкретних рекомендаціях, спрямованих на покращення використання систем цифрової ідентифікації в публічному управлінні, що можуть слугувати основою для практичного впровадження та оптимізації адміністративних процедур та публічних послуг.

*Апробація наукових досліджень.* Основні результати дослідження були представлені та обговорені на наукових конференціях: XII Всеукраїнська студентська науково-практична конференція «Актуальні проблеми ефективного соціально-економічного розвитку України: пошук молодих», (м. Вінниця, ВТЕІ ДТЕУ 20 квітня 2023 року), тема статті «Особливості процесу цифровізації публічного управління в Україні»; X Всеукраїнська науково-практична Інтернет-конференція «Менеджмент XXI століття: Сучасні моделі, стратегії, технології» (м. Вінниця, ВТЕІ ДТЕУ 10 жовтня 2023 року), тема статті «Роль цифрової ідентифікації у публічному управлінні та адмініструванні в процесі відновлення України: виклики та перспективи».

Робота містить 55 сторінок тексту, 28 рисунків та 4 додатки. У кваліфікаційній роботі використано 59 джерел.

## РОЗДІЛ 1

### КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА РОЛЬ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ У ПУБЛІЧНОМУ УПРАВЛІННІ

Електронна ідентифікація – це процедура використання ідентифікаційних даних особи у електронному форматі для однозначного визначення фізичних осіб, юридичних осіб або представників фізичних і юридичних осіб. Дозвіл на використання технологій для ідентифікації платників податків в їхньому електронному кабінеті встановлюється центральним органом виконавчої влади, відповідальним за формування та впровадження державної фінансової політики. [5]

Термін «Цифрова ідентифікація» (Digital Identification або Digital ID) виник у контексті розвитку технологій та потреби в ефективних методах ідентифікації та аутентифікації осіб у цифровому середовищі.[5]

Цифрова ідентифікація виникла у відповідь на ростучу потребу в забезпеченні безпеки та ідентифікації користувачів в онлайн-середовищі. Цей термін почав набирати популярності у 1990-2000-х роках відповідно до розвитку Інтернету та інших цифрових технологій. Однак важливо відзначити, що поняття ідентифікації і аутентифікації, які є складовими частинами цифрової ідентифікації, існували задовго до настання епохи цифрових технологій і використовувалися у фізичних системах безпеки та контролю доступу. З появою Інтернету та зростанням обсягу цифрових даних, ці поняття стали важливими для онлайн-ідентифікації та забезпечення безпеки в цифровому світі.

Україна розробила "Інтегровану систему електронної ідентифікації," яка представляє собою інформаційно-телекомунікаційну систему, призначену для забезпечення зручної, доступної та безпечної електронної ідентифікації та аутентифікації користувачів системи. Ця система також спрямована на забезпечення сумісності та інтеграції схем електронної ідентифікації та їх взаємодії з офіційними веб-сайтами, інформаційними системами органів державної влади,



органів місцевого самоврядування, юридичних осіб та фізичних осіб - підприємців. Також ця система має захищати інформацію та особисті дані шляхом використання єдиних вимог, форматів, протоколів та класифікаторів, а також задовольняти інші потреби, визначені законодавством. [14]

У положенні щодо інтегрованої системи електронної ідентифікації зазначено, що основна мета цієї системи полягає в тому, щоб надати користувачам доступ до електронних послуг та сервісів, які надаються державними органами, місцевими органами влади, юридичними особами та фізичними особами-підприємцями відповідно до схем електронної ідентифікації. Крім того, ця система підтримує ефективний електронний документообіг та сприяє проведенню інших видів діяльності з використанням електронної ідентифікації.

Інтегрована система електронної ідентифікації відіграє важливу роль у структурі інформаційно-телекомунікаційного середовища, сприяючи ефективній електронній взаємодії між суб'єктами взаємодії та користувачами системи. Вона забезпечує проведення необхідних процедур та електронну ідентифікацію користувачів для надання їм електронних послуг та доступу до сервісів. Також система взаємодіє та сумісна з іншими інформаційно-телекомунікаційними системами, які реалізують схеми електронної ідентифікації, і забезпечує дотримання вимог законодавства щодо захисту інформації та персональних даних. Крім того, система розвивається у напрямку інтеграції з інформаційно-телекомунікаційними системами для транскордонної електронної ідентифікації і інтегрує інформаційно-телекомунікаційні системи суб'єктів взаємодії до своєї структури. [14]

Цифрова ідентифікація в публічному управлінні визначається різними факторами і залежить від контексту та конкретних обставин.

На наявність і роботу систем цифрової ідентифікації впливає наявність відповідного законодавства та політичної волі. Закони повинні регулювати, як збирається, зберігається та використовується особиста інформація. Вони також повинні визначити, які види ідентифікації є законними. Зростаюча доступність і розвиток цифрових технологій, таких як біометрика, блокчейн і шифрування,

впливає на можливості реалізації цифрової ідентифікації. Забезпечення безпеки та захисту персональних даних є життєво важливим. Незахищені системи ідентифікації можуть зашкодити приватності та кіберзлочинності.

Також, потрібно врахувати доступність і зручність для громадян, тобто громадяни повинні бути в змозі використовувати системи цифрової ідентифікації та вважати їх зручними. Вони повинні бути надзвичайно зручними у використанні та підтримувати високу якість обслуговування.

Різні організації та органи влади повинні мати відповідну інфраструктуру, стандарти та протоколи обміну інформацією, щоб використовувати цифрову ідентифікацію.

Розвиток і підтримка систем цифрової ідентифікації часто вимагає значних інвестицій. На швидкість та масштаб реалізації таких систем впливає наявність фінансування.

Також, треба зазначити, що люди повинні бути впевнені, що система цифрової ідентифікації безпечна та надійна.

Якщо країна хоче обмінюватися інформацією з іншими країнами або співпрацювати на міжнародному рівні, важливо враховувати міжнародні стандарти та вимоги до цифрової ідентифікації.

Особливі потреби та зобов'язання влади і8 суспільства також впливають на впровадження систем цифрової ідентифікації. Наприклад, можуть вимагатися різні рішення щодо ідентифікації в різних областях, таких як охорона здоров'я, соціальні послуги та податки.

Загалом, цифрова ідентифікація в публічному управлінні є складним завданням, яке враховує багато факторів, і його успіх залежить від збалансованості цих факторів у контексті конкретної країни та цілей влади.

Базові ідеї, методи та принципи, які лежать в основі розуміння та розвитку цифрової ідентифікації, представлені в теорії цифрової ідентифікації. Деякі ключові теоретичні ідеї, які використовуються в цій галузі, такі: Ідентифікація та аутентифікація: ця ідея описує процес визначення людини або предмета та підтвердження того, що вони справді є ними. Вона описує різні способи, за



допомогою яких системи ідентифікують користувачів, наприклад за допомогою паролів, біометричних даних і одноразових кодів.

Цифрова безпека – це дії, спрямовані на запобігання несанкціонованому доступу, крадіжки чи злому цифрових ідентифікаторів і персональних даних. Це охоплює технологічні, організаційні та юридичні аспекти цифрової безпеки.

Електронний документ та цифровий підпис: ця ідея стосується використання цифрових підписів і електронних документів для підтвердження автентифікації та ідентичності. Вона охоплює юридичні та технічні питання використання цих інструментів.

Системи ідентифікації на основі біометрії: це те, що використовує біометричні дані, такі як відбитки пальців або розпізнавання обличчя, для ідентифікації людей. Вона розглядає як технології, так і моральні проблеми, пов'язані з цим типом ідентифікації.

Правові аспекти цифрової ідентифікації: ця ідея розглядає закони, які регулюють використання цифрових ідентифікаторів і визначають права та обов'язки громадян і організацій, які їх використовують.

Цифрова ідентичність та саморегуляція: це концепція, яка охоплює питання про те, як люди та організації можуть самостійно контролювати свою цифрову ідентичність, а також про те, як системи цифрової ідентифікації можуть зробити більш зрозумілими для користувачів і більш прозорими.

Для розробки рекомендацій і політики в галузі цифрової ідентифікації та публічного управління необхідні ці теоретичні ідеї, щоб зрозуміти та покращити системи цифрової ідентифікації.

Серед основних факторів, які впливають на процес цифровізації державного управління та цифрової трансформації суспільства в зарубіжних країнах, можна виділити наступне: особливості ринкової економіки, які проявляють себе у збільшенні свободи підприємництва, вільного руху робочої сили та конкурентності на ринку праці; розвиток громадянського суспільства та соціального партнерства в цифровому середовищі; децентралізація влади та впровадження ефективних структурних і регіональних політик [37].

Впровадження цифрової ідентифікації в публічному секторі є актуальним напрямком для багатьох країн у світі. Нижче подано приклади досвіду з різних країн та успішних проєктів:

Естонія: Естонія відома своєю інноваційною системою електронного громадянства (e-residency). Ця програма надає іноземцям можливість отримати цифровий ідентифікаційний номер та користуватися цифровими послугами країни, включаючи відкриття бізнесу. Естонська цифрова ідентифікація базується на картах ID-карт та мобільних ID. [52] Цифрові посвідчення особи мають 98% естонців, які використовують їх для банківських транзакцій, електронного голосування, медичного страхування, онлайн-підписів і сплати податків. Естонці в середньому економлять 5 робочих днів на рік завдяки цим технологіям. [46] Електронне резидентство привернуло фрілансерів і підприємців з усього світу до державних цінностей і вірувань, створивши мережу людей, які захоплюються Естонією та ототожнюють себе з нею.

Індія: Уряд Індії запустив програму Aadhaar, яка надає біометричні ідентифікаційні номери для громадян. Aadhaar став ключовим інструментом для надання субсидій та соціальних послуг. Ця програма дозволила спростити та забезпечити більший доступ до державних послуг.[58]

Швеція: Швеція впровадила BankID – це електронне посвідчення особи, що шведською також називають «e-legitimation». BankID — це простий спосіб підтвердити свою особу, наприклад для укладання контрактів та електронного підпису платежів в інтернеті. Електронний підпис через BankID накладає юридичні обов'язки так само, як і фізичний підпис.[55]

Сінгапур: Понад 3,8 млн людей у Сінгапурі використовують SingPass, унікальну цифрову ідентифікацію, щоб отримати доступ до більш ніж 300 державних онлайн-сервісів. Відповідний мобільний додаток підтримує біометричну двофакторну верифікацію за допомогою розпізнавання відбитків пальця та обличчя. SingPass Mobile є частиною національної програми цифрової ідентичності уряду Сінгапуру, яка спрямована на те, щоб зробити більш зручним і безпечним для громадян робити покупки в Інтернеті.[46]

Канада: Крім того, Канада розробляє Pan-Canadian Trust Framework, федеральну схему цифрової ідентифікації, яку пілотує Канадська рада з автентифікації цифрових ідентифікаторів, некомерційна організація (DIACC). Восени 2018 року розпочався національний проєкт перевірки ідеї єдиної служби автентифікації Sign In Canada.[59]

Бельгія: У Бельгії кожен громадянин віком від 12 років повинен мати електронне посвідчення, яке ідентифікує особу та дозволяє використовувати електронний підпис. Підписувати документи та електронні листи, виписувати рахунки, укладати контракти та багато іншого можна зробити за допомогою е-посвідчення. [46]

Австрія: Смарт-карта громадянина eID має кілька функцій: вона служить офіційним посвідченням особи, служить електронним ідентифікатором для IT-процесів, додає електронний підпис до документів і електронних листів і може використовуватися як система контролю доступу. Коли eID використовується як картка громадянина, державні службовці можуть використовувати його, щоб ідентифікувати себе як зареєстрованого користувача послуг електронного уряду як приватну особу, так і офіційно. [57]

Україна: Наразі в Україні електронна ідентифікація здійснюється за допомогою таких інструментів, як електронний підпис, BankID і MobileID. Ці інструменти дозволяють користувачам користуватися цифровими послугами, мобільним застосунком і порталом «Дія» або «е-документообіг». [46]

Ці приклади демонструють різноманітність методів цифрової ідентифікації в публічному секторі та те, наскільки вони ефективно працюють, щоб спростити для громадян отримання державних послуг і підвищити ефективність управління.

Загалом, для України, молодій демократичній країні, важливо вивчити, як змінюються моделі управління розвинутих держав. Тим не менш, основні елементи трансформаційного періоду змусили створити нову систему державного регулювання. Економіка зазнала значних структурних деформацій, оскільки більшість інституцій, необхідних для функціонування ринку, відсутні в державі. [24]. Це дозволяє людям брати участь у вирішенні проблем, які стосуються їхнього



регіону. Іншими словами, громадяни мають право законно контролювати функціонування цих органів. Це сприяє розвитку громадянського суспільства та створенню ефективного місцевого самоврядування в країні. [43]

ПриватБанк вже впровадив проект верифікації клієнтів у банківській сфері, який базується на поведінковій автентифікації та прозорій біометрії. Це підвищує надійність і безпеку клієнтів онлайн-банкінгу та мобільного додатку «Приват24». На платформі «NuDetect» компанії «MasterCard» працює цифрове рішення на основі AI-технологій, яке дозволяє перевіряти унікальність поведінки клієнтів, аналізуючи їхні характеристики, пасивні біометричні та поведінкові показники під час взаємодії з пристроями та додатками. [29]

Постійний аналіз поведінки та історії користування аккаунтом кожного користувача в режимі реального часу дозволяє оцінювати ризики, прогнозувати можливі вторгнення та запобігати кібератакам. Н. Кангін, керівник напряму впровадження цифрових послуг «Mastercard» в Україні, зазначає, що «платформа «NuDetect» створює профайл клієнта, в якому збираються понад 300 його унікальних параметрів за допомогою машинного навчання». [40].

Крім того, «ПриватБанк» встановив в торгових точках перші в Україні біометричні POS-термінали «Android PAX», які оснащені технологією «FacePay24», яка надає можливість оплати обличчям. Для використання «оплати обличчям» потрібно встановити програму «Privat24» на своєму мобільному телефоні. Потім потрібно зробити три фотографії з різних ракурсів і підключити банківську карту. База даних FacePay24 базується на системі розпізнавання обличчя Amazon Rekognition і забезпечує безпеку даних клієнтів банку за допомогою шифрування, технічного і фізичного контролю. [39].

В Україні система електронних послуг і електронної ідентифікації розвивається швидкими темпами. Це включає створення порталу державних послуг «Дія» під егідою профільного міністерства, запуск Інтегрованої системи електронної ідентифікації, впровадження технології SmartID і процес оптимізації електронних реєстрів даних. Це створило значний поштовх для розвитку міжнародної співпраці в цій галузі. Під час засідання Комітету Ради асоціації ЄС-

Україна Україна подала запит щодо взаємного визнання довірчих послуг у відповідності зі статтею 14 Регламенту eIDAS. За допомогою проєкту EU4Digital Україна стала однією з країн Східного Партнерства та отримала запрошення взяти участь у пілотних проєктах по створенню транскордонних систем електронного підпису, які включають транскордонне визнання електронних підписів і інструменти електронної ідентифікації. У виборі брали до уваги адаптацію законодавства України та технічну реалізацію вимог щодо електронних довірчих послуг. [47]

В сучасному інформаційному суспільстві цифрові технології, як і будь-які попередні досягнення науково-технічної революції, дають можливості для покращення роботи органів публічної влади і неодмінно стають невід'ємною частиною нашого життя [38]. Цифрова трансформація впливає на різні сфери, включаючи публічне управління і взаємодію між громадянами та владою. Одним із ключових аспектів цієї трансформації є цифрова ідентифікація, яка дозволяє ідентифікувати особу в електронному середовищі та забезпечує доступ до різних цифрових послуг та ресурсів.

Цифрова ідентифікація, яка полягає в підтвердженні особи громадян через цифрові засоби, може бути важливою складовою цифрової трансформації муніципального управління. Так як забезпечує безпеку та конфіденційність даних при користуванні електронними послугами муніципального управління, допомагає створювати безпечні електронні підписи та перевіряти автентичність документів, підтверджує особу громадян, коли вони звертаються за муніципальними послугами, допомагає муніципалітетам збирати та аналізувати дані для покращення надання послуг та прийняття рішень на основі даних.

Таким чином, цифрова ідентифікація впливає на різні аспекти муніципального управління і сприяє його цифровій трансформації. Вона забезпечує ефективність, безпеку та відкритість муніципального управління, полегшуючи взаємодію з громадянами та покращуючи якість наданих послуг.[26]

Але цифрова ідентифікація не обмежується лише технічними аспектами. Вона також пов'язана з публічним контролем, прозорістю та громадською участю у владних процесах.

В проєкті Закону України «Про публічний контроль» від 6 липня 2015 року № 2297-а [24] було зазначено, що публічний контроль є діяльністю суб'єктів публічного контролю з нагляду, перевірки й оцінки діяльності об'єктів публічного контролю на предмет відповідності такої діяльності вимогам, встановленим законодавством України, та інтересам територіальної громади, в якому також підкреслено, що нагляд є однією із складових публічного контролю. [23]

Результати опитування, проведеного Національним демократичним інститутом, показали, що 94% українців вважають, що Україна повинна стати повноцінною демократією, де основними елементами є прозорість і підзвітність уряду, представництво інтересів громадян і функціонування демократії. [35].

Тобто, в сучасному демократичному суспільстві важливим компонентом є публічний контроль влади з метою досягнення балансу між її діями та відповідальністю перед громадськістю. Також публічний контроль запобігає порушенню існуючих правових норм з боку органів державної влади та прийняттю посадовцями передчасних, упереджених, необґрунтованих рішень, вчиненню дій, які є наслідком створення неякісного законодавства. [23]

Державна влада та її апарат покликані виконувати суспільно-регулятивні функції на основі законів; їх основна мета полягає в тому, щоб гарантувати стабільне існування держави та суспільства. Таким чином, публічна служба має стати основою для того, щоб українське суспільство могло входити до світового співтовариства та розвивати свою ідентичність як повноправної європейської та світової держави. Уся діяльність управлінського апарату та кадрова політика країни мають бути спрямовані на те, щоб зберегти національну державність у світлі глобалізаційних і інтеграційних тенденцій, забезпечити стабільність і розвиток суспільства.[42]



Міністерство цифрової трансформації України (Мінцифра) є державним органом, відповідальним за реалізацію політики Уряду щодо відкриття найбільш важливих для суспільства даних. Відкриті дані мають потужний антикорупційний ефект, сприяють прозорості влади, позитивно впливають на розвиток економіки.[13]

Основним законом щодо врегулювання відносин у сферах надання електронних довірчих послуг та електронної ідентифікації є: Закон України «Про електронні довірчі послуги» — документ 2155-VIII, чинний, поточна редакція — Редакція від 01.01.2023, підстава — 2801-IX. Цей закон регулює правові та організаційні питання надання електронних довірчих послуг, включаючи права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, а також порядок державного нагляду за дотриманням вимог законодавства у сфері електронних довірчих послуг.

Цифрова ідентифікація, поєднана з можливістю зберігання документів та інших ідентифікаційних даних держави в смартфоні, відкриває безліч можливостей для спрощення процесів взаємодії громадян з державою та інших організацій.

Мета створення ідеї «Держава у смартфоні» полягає в бажанні швидко вирішувати різноманітні соціальні та адміністративні проблеми. Це не просто звичайне оцифровування адміністративних послуг, це стосується створення єдиної державної платформи, яка захистить права та інтереси кожної людини та громадянина, систематизуючи та об'єднуючи всі дані з реєстрів.[35] Концепція «держави у смартфоні» описує систему, яка складається з електронного урядування, кібернетичної безпеки, електронного бізнесу, судів, електронних систем охорони здоров'я, електронної освіти, розумних міст, електронного транспорту та повсюдного доступу до Інтернету.[21]

Ця інтеграція дозволяє громадянам зручно та безпечно підтверджувати свою особу онлайн, використовуючи біометричні дані, такі як відбитки пальців або розпізнавання обличчя на їхніх смартфонах. Це важливо для проведення різноманітних транзакцій, таких як електронний голосування, отримання медичних рецептів або підписування юридичних документів.

Система "eHealth" [54] та портал "Helsi.Me" [56] в Україні відіграють важливу роль у забезпеченні доступу до якісних медичних послуг та демонструють фундаментальну цінність життя та здоров'я громадян. Однак для забезпечення безпеки та конфіденційності медичних даних у цих системах, цифрова ідентифікація грає важливу роль.

Ідентифікація в цих системах полягає у визначенні особи, яка звертається за медичною допомогою чи доступом до своїх медичних записів. Цифрова ідентифікація використовується для підтвердження особи пацієнта та забезпечення безпеки його медичної інформації.

Загалом, ця інтеграція робить взаємодію з державою та іншими організаціями більш зручною, безпечною та ефективною, спрощуючи процеси ідентифікації та доступу до різних послуг та ресурсів.

Відносини, пов'язані з наданням електронних довірчих послуг та електронною ідентифікацією, регулюються Конституцією України [3], Цивільним кодексом України [4], законами України "Про інформацію" [10], "Про захист інформації в інформаційно-комунікаційних системах" [8], "Про електронні документи та електронний документообіг" [7], "Про захист персональних даних" [9], цим Законом, а також іншими нормативно-правовими актами.

Статті, в яких йдеться про цифрову ідентифікацію в Законі України «Про електронні довірчі послуги» зазначено у додатку А.

У звіті Міністерства цифрової трансформації України за 2022 рік збільшено кількість транзакцій інтегрованої системи електронної ідентифікації (ICEI) на 141% до 29 млн (12 млн у 2021 році) та сформовано більше 13,7 млн кваліфікованих сертифікатів електронних підписів користувачів електронних довірчих послуг.

З метою наближення національного законодавства щодо електронної ідентифікації та електронних довірчих послуг до європейських вимог Мінцифри Верховна Рада схвалила проект Закону України «Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних

довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації». [20]

Для дослідження відношення громадян до цифрової ідентифікації в публічному управлінні було використано різноманітні методи дослідження:

1. Проведено анкетування серед громадян в Google-формах, де створено запитання, що стосуються їхнього відношення до цифрової ідентифікації та її використання.
2. Організовано кілька фокус-груп, де невелика група громадян обговорювала питання, пов'язані з цифровою ідентифікацією. Цей метод дозволив отримати глибше розуміння відношення та поглядів учасників.
3. Досліджено офіційні документи, звіти, законодавства і рішення, які стосуються цифрової ідентифікації та її регулювання в Україні.
4. Проаналізовано опитування і статистичні дані.
5. Досліджено існуючу літературу та проаналізовано документи, які стосуються моїх дослідницьких питань.



## РОЗДІЛ 2

### АНАЛІЗ СУЧАСНОГО СТАНУ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ В УКРАЇНІ ТА ЇЇ ВПЛИВ НА РОЗВИТОК ПУБЛІЧНОГО УПРАВЛІННЯ

#### 2.1 Правові засади діяльності та організаційно-функціональна характеристика Міністерства цифрової трансформації України

Дослідження було проведено з метою залучення України до європейського цифрового ринку. Мета опитування полягала в тому, щоб дізнатися думки стейкхолдерів щодо процесів розвитку цифрової економіки в Україні. Опитування включало 18 експертів із різних галузей цифровізації, які представляли наукові та освітні спільноти, органи влади, бізнес і громадські експертизи. Загальна оцінка процесів цифрового розвитку в Україні за останні півтора роки є переважно позитивною, як показано на рис. 2.1. [47]

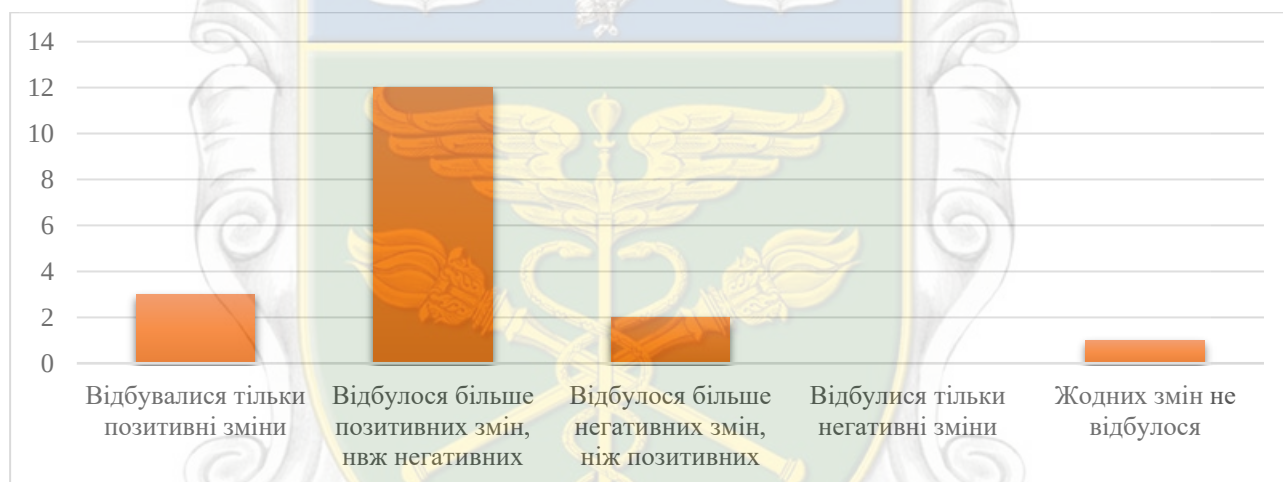


Рисунок 2.1. – Відповіді на питання експертного опитування «Як ви оцінюєте процеси цифрового розвитку України за останні півтора роки?»

Динамічний розвиток цифрової економіки та швидке впровадження цифрових технологій в усі сфери суспільства і господарства викликають як позитивні, так і негативні наслідки. Ця ситуація виокремлюється протиріччями та неоднозначністю, які можуть бути спрощено описані як «порушення логіки причин і наслідків».

З одного боку, цифрова трансформація принесла значні позитивні зміни, включаючи підвищення продуктивності, зручність та доступність послуг, зниження витрат та розвиток нових галузей бізнесу. Вона стала важливим інструментом для підвищення конкурентоспроможності країн та покращення якості життя громадян.

З іншого боку, цифровий революційний розвиток супроводжується викликами та негативними наслідками, такими як кіберзагрози, витоки особистих даних, синергетика фінансових криз, вплив на робочі місця та безпеку праці, а також загрози інформаційної безпеки та кібернетичні конфлікти. Поширення дезінформації та інформаційних воєн також є серйозними викликами для сучасного світу.

Отже, вирішення проблем, пов'язаних із цифровою трансформацією, вимагає балансу між позитивними та негативними аспектами, а також тісної співпраці між наукою, бізнесом та владою. Належна увага до захисту даних, кібербезпеки та етичних питань стає надзвичайно важливою в умовах швидкого цифрового розвитку. [33]

Міністерство цифрової трансформації України є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України.[13]

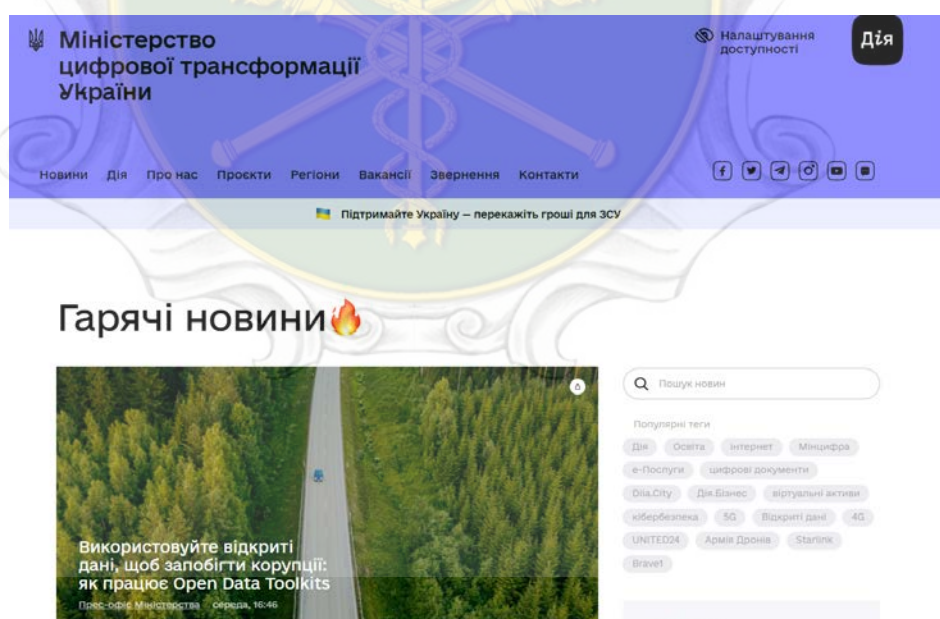


Рисунок 2.2 – Веб-сайт Міністерства цифрової трансформації України

Склад апарату Міністерства цифрової трансформації України (Наказ Мінцифри від 26.04.2021 № 71/к) зазначено нижче на рисунку 2.3, детальніший склад розміщено в додатку Б.



Рисунок 2.3 – Склад апарату Міністерства цифрової трансформації України



Проведемо аналіз даних на офіційному сайті Міністерства цифрової трансформації України, результати якого на рис. 2.4 та 2.5. [16-19]

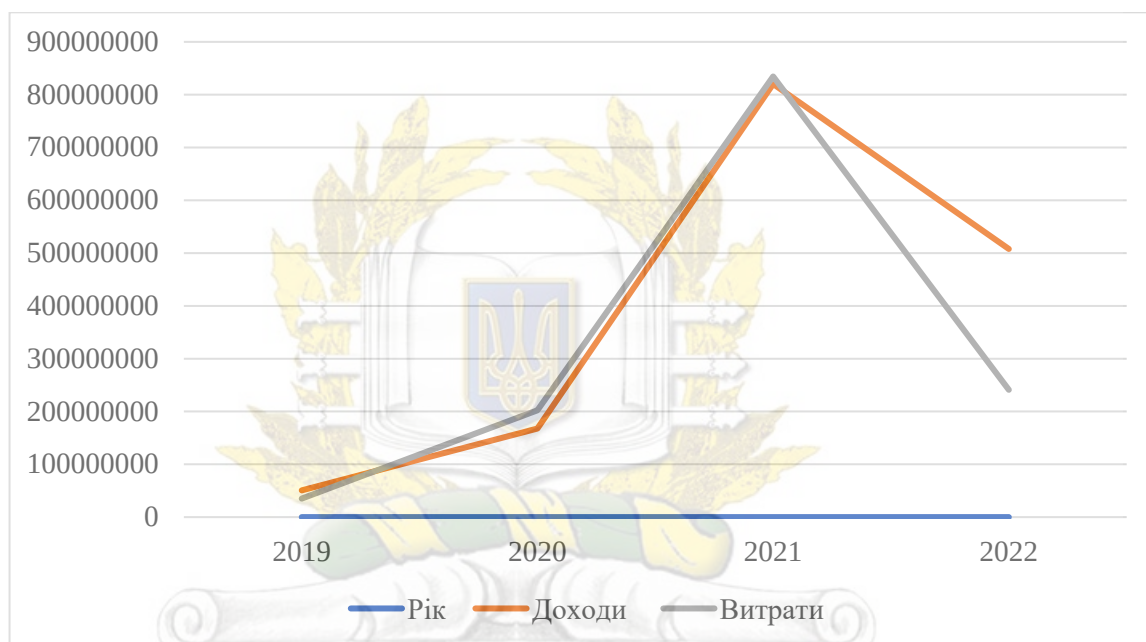


Рисунок 2.4 – Доходи та витрати фінансової діяльності Міністерства цифрової трансформації України за звітний період

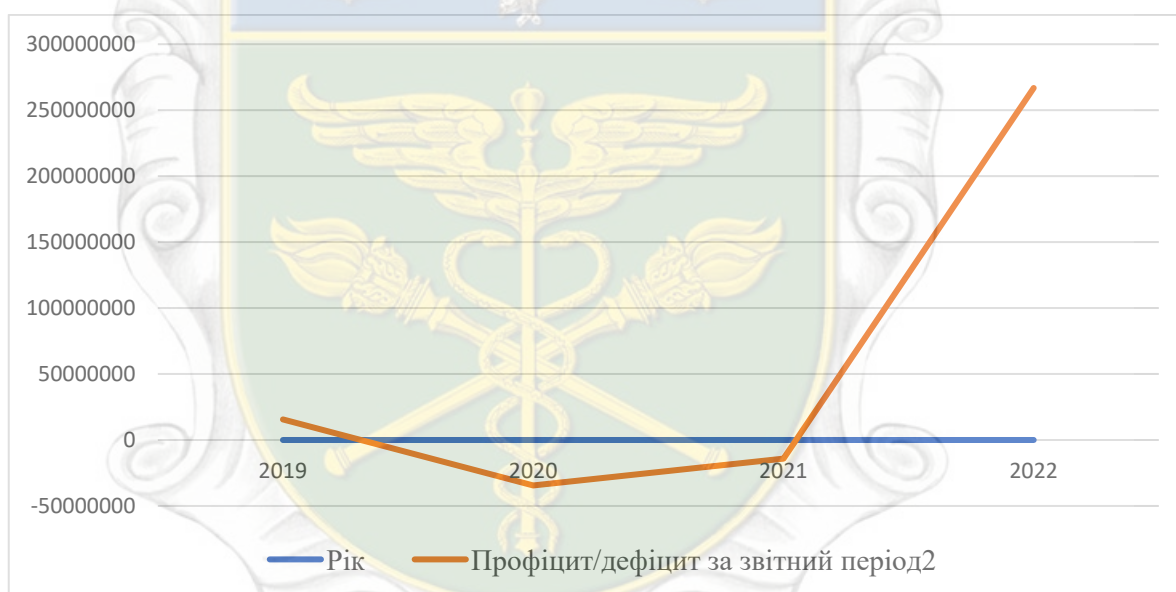


Рисунок 2.5 – Профіцит/дефіцит фінансової діяльності Міністерства цифрової трансформації України за звітний період

Більшість компонентів е-урядування схильні до загроз, які виникають під час мережевої війни, як зовнішньої, так і внутрішньої. Отже, пріоритетним завданням має бути створення національної системи ідентифікації, яка відповідатиме

сучасним світовим стандартам. Зважаючи на те, що Україна обрала шлях європейської інтеграції, доцільно дотримуватися правил Регламенту eIDAS. Намагання Державного агентства України з питань розвитку електронного урядування розробити «Стратегію впровадження сучасних засобів та схем електронної ідентифікації в Україні» є позитивним кроком у цьому напрямку. Слід зазначити, що кожна країна проходить свій власний шлях створення електронного урядування, оскільки кожна країна має різні ментальні, матеріальні, технологічні та економічні ресурси. З кожним роком зростає кількість країн, які активно використовують е-урядування.

Відповідно до Положення про Єдиний державний веб-портал електронних послуг: Постанова Кабінету Міністрів України від 4 грудня 2019 р. № 1137, щодо цифрової ідентифікації Портал Дія має такі функції:

1) електронна ідентифікація та автентифікація користувачів за допомогою інтегрованої системи електронної ідентифікації, кваліфікованих електронних підписів і печаток, а також інших засобів ідентифікації; забезпечення віддаленої ідентифікації фізичних осіб (без їх особистої присутності) за допомогою мобільного додатка Порталу Дія (Дія) з метою безоплатного надання кваліфікованих електронних довірчих послуг, пов'язаних з використанням віддаленого кваліфікованого електронного підпису “Дія.Підпис” (“Дія ID”);

2) за допомогою веб-порталу можна завантажити, заповнити та подати заяви та інші документи завдяки інтегрованій системі електронної ідентифікації, кваліфікованого електронного підпису або печатки або інших засобів електронної ідентифікації, які дозволяють визначити особу заявника;

3) взаємодія між різними системами, такими як інтегрована система електронної ідентифікації, системи електронної взаємодії електронних інформаційних ресурсів держави та органів виконавчої влади, а також системи електронного документообігу суб'єктів розгляду звернень; можливість отримання відомостей про показники якості послуг через ці системи [12].

Основними цілями Міністерства цифрової трансформації до 2024 року є:

1. Забезпечити 100% доступність публічних послуг онлайн , тобто всі публічні послуги повинні бути доступні громадянам та бізнесу через інтернет без будь-яких перешкод.

2. Забезпечити 95% покриття швидкісним інтернетом для населення, соціальних об'єктів і головних автошляхів. Це передбачає, що майже всі жителі країни, соціальні заклади та важливі транспортні маршрути мають доступ до швидкого Інтернету.

3. Залучити 6 мільйонів українців до програми розвитку цифрових навичок. Ця ціль вказує на значний розвиток цифрової грамотності серед населення, що допоможе людям використовувати цифрові технології більш ефективно.

4. Збільшити долю ІТ у ВВП країни до 10%: Це значить, що інформаційні технології стануть більшим фактором у валовому внутрішньому продукті країни. [48]

## 2.2 Основні проблеми та виклики функціонування цифрової ідентифікації

Було проведено 2 фокус-групи на теми: «Відношення громадян до впровадження цифрової ідентифікації» та «Сприйняття громадян щодо безпеки та конфіденційності в ідентифікаційних системах».

Крім того, було проведено опитування громадської думки щодо цифрової ідентифікації, що пройшли 97 людей. Для початку аналізу поділили учасників на вікові групи (рис. 2.6).

В свою чергу, результати опитування на рис. 2.7 свідчать про різноманітність рівнів інформованості щодо цифрової ідентифікації серед учасників. На перший погляд, важко визначити домінуючий тренд, оскільки спостерігається різниця в оцінках.



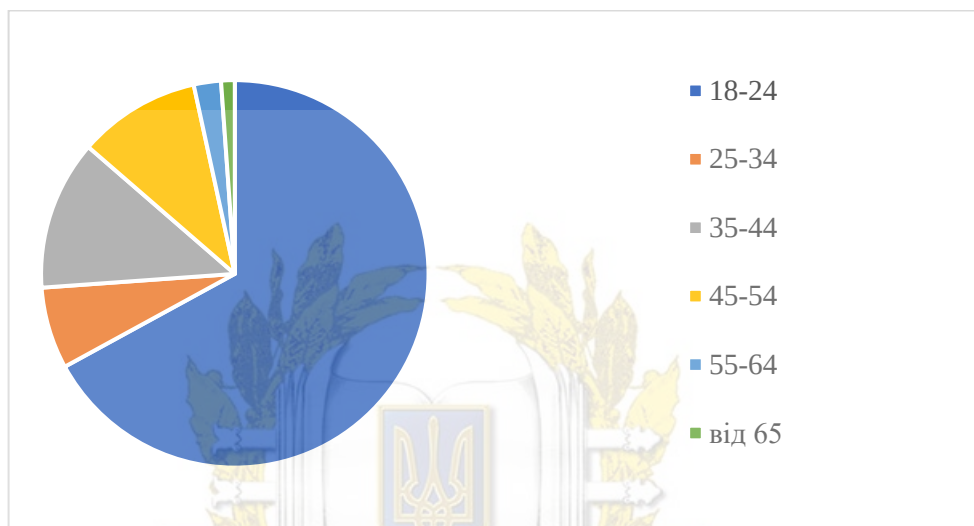


Рисунок 2.6 – Розподіл відношення до цифрової ідентифікації за віковими групами

Не виявлено осіб із дуже слабким рівнем інформованості, що може свідчити про загальний мінімальний рівень усвідомлення даної теми серед учасників. Однак невелика кількість опитаних визнала свій слабкий рівень, вказуючи на наявність осіб, які можуть виявитися більш зацікавленими в інформаційному підході.

Більшість опитаних оцінили свою інформованість як середню чи добру. Це може свідчити про наявність основного рівня інтересу та визнання теми, але також вказує на потребу подальшого удосконалення знань.

Група осіб, які визнали свій рівень інформованості як відмінний, свідчить про наявність досвідчених та добре обізнаних у цифровій ідентифікації учасників.

Загалом, результати вказують на важливість надання додаткової інформації та освіти, особливо серед тих, хто оцінив свій рівень менш як "відмінний".

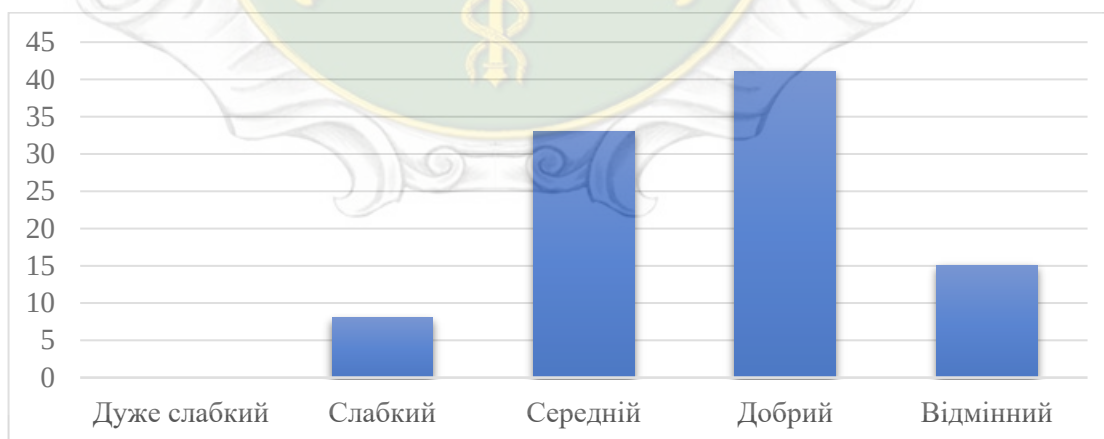


Рисунок 2.7 – Свій рівень інформованості щодо цифрової ідентифікації

Результати опитування на рис. 2.8 вказують на різноманіття переконань учасників щодо рівня інформованості населення в Україні з питань цифрової ідентифікації.

Деякі учасники вважають, що рівень інформованості високий, що може свідчити про існування групи осіб, які вже добре розуміють та цікавляться цифровою ідентифікацією. Інші вважають його середнім, вказуючи, що багато людей володіють базовими знаннями, але можуть вигідно розширити їх. Є також ті, хто вбачає низький рівень інформованості, що може вказувати на важливість підвищення рівня інформаційної грамотності в цій області.

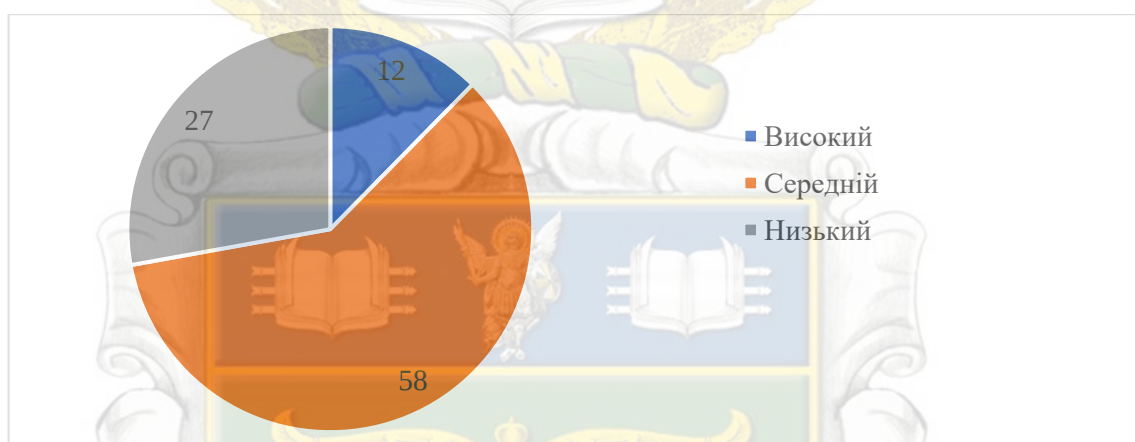


Рисунок 2.8 – Сприйняття про рівень загальної інформованості населення про цифрову ідентифікацію в Україні

У результаті аналізу відповідей учасників на рисунку 2.9 виявлено, що у частини опитаних існує велика різноманітність щодо частоти прочитання новин чи статей про цифрову ідентифікацію. Одні учасники вказали, що звертають увагу на цю тему щодня, що може свідчити про активний інтерес та високий рівень освіченості. Інші, зі значною кількістю відповідей, визнали, що роблять це кілька разів на тиждень, вказуючи на помірний рівень уваги до даного питання. Зауважено також, що значна кількість учасників опитування рідко звертається до матеріалів про цифрову ідентифікацію, що може свідчити про загальний низький інтерес або відсутність регулярного стеження за цією темою серед даної групи. Такий розмаїтий підхід до частоти прочитання вказує на необхідність розробки збалансованих інформаційних стратегій для різних груп аудиторії.

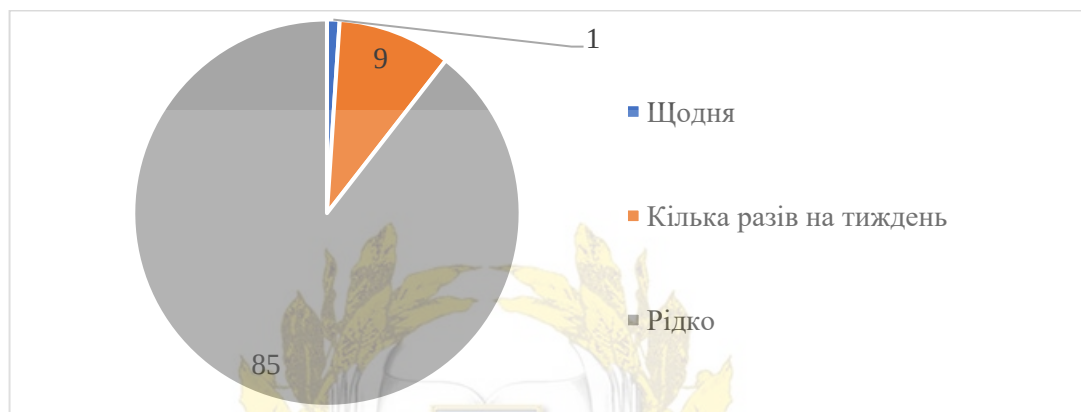


Рисунок 2.9 – Частота прочитання новин або статей про цифрову ідентифікацію

У розгляді участі в навчальних заходах чи інформаційних кампаніях (рис. 2.10), повідомлено, що частина опитаних бере участь в таких заходах — це свідчить про активний інтерес до питань цифрової ідентифікації та бажання розширити свої знання в цій області. Тим часом, значна кількість відповідей "Ні" може вказувати на відсутність зацікавленості або доступу до таких заходів у певних груп населення. Додатково, значна кількість вказали "Поки що ні, але планую", що свідчить про потенційний інтерес до майбутніх навчальних ініціатив. Це підкреслює важливість розробки та проведення доступних та привабливих навчальних заходів для всіх груп населення.

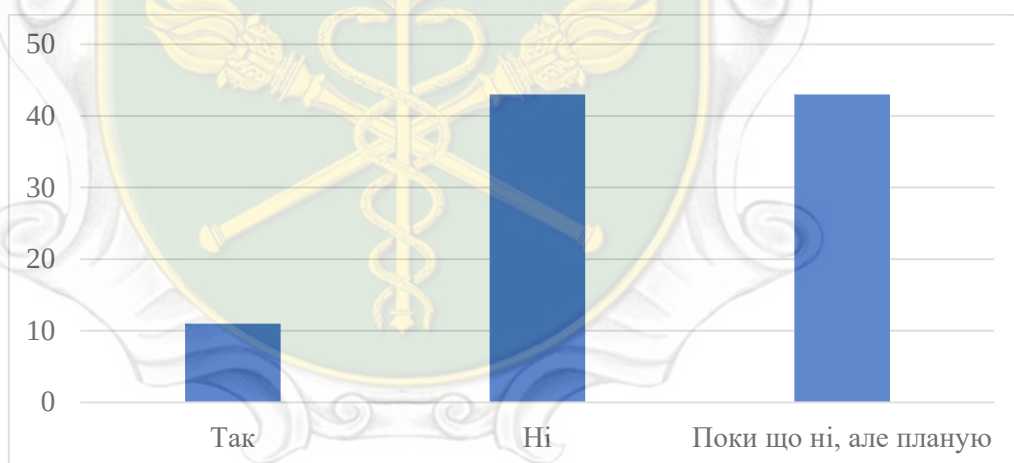


Рисунок 2.10 – Участь у навчальних заходах чи інформаційних кампаніях, що стосуються цифрової ідентифікації

За результатами дослідження (рис. 2.11) найпопулярніші джерела отримання інформації про цифрову ідентифікацію визначено як новинні сайти, офіційні



джерела (урядові та корпоративні веб-сайти) та соціальні мережі. Зазначено, що значна кількість респондентів вказала на соціальні мережі як основний інформаційний канал, що може відзначати активний обмін думками та інформацією в цьому середовищі. Офіційні джерела також мають велику вагу, що свідчить про довіру до інформації, яку надають уряд та корпорації. Ці результати дозволяють визначити стратегії поширення інформації про цифрову ідентифікацію, зокрема залучення соціальних мереж та офіційних ресурсів.

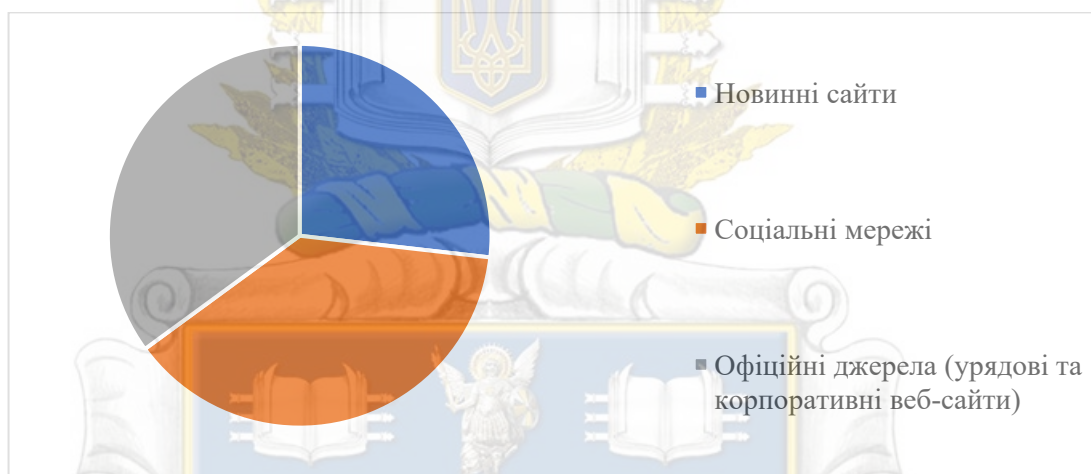


Рисунок 2.11 – Найпопулярніші джерела отримання інформації про цифрову ідентифікацію

Внаслідок аналізу відповідей (рис. 2.12) стосовно основних переваг використання цифрової ідентифікації виокремлено декілька ключових аспектів. Зазначено, що для більшості респондентів основними перевагами є зручність та швидкість, що свідчить про прагматичний підхід та оцінку ефективності використання цифрових ідентифікаторів. Зменшення бюрократичних процедур, безпека та зменшення ризику втрати документів також визнаються як значущі фактори. Важливо відзначити, що лише невелика кількість респондентів визнає, що використання цифрової ідентифікації порушує права і свободи людини. Це підкреслює загальний позитивний ставлення до впровадження цифрових технологій в області ідентифікації.



Рисунок 2.12 – Основні переваги у використанні цифрової ідентифікації

Аналізуючи основні недоліки на рис. 2.13 у використанні цифрової ідентифікації, виокремлено кілька ключових аспектів. Більшість респондентів вказали на ризик несанкціонованого доступу до даних, що свідчить про загальне занепокоєння стосовно безпеки особистої інформації. Проблеми з конфіденційністю та приватністю також визнаються як серйозний недолік, відзначаючи важливість забезпечення захисту особистих даних під час впровадження цифрових ідентифікаторів. Крім того, технічні проблеми та збої систем також є серйозним викликом, який може вплинути на надійність та стабільність використання цифрової ідентифікації. Це підкреслює необхідність розробки ефективних стратегій для запобігання та вирішення цих проблем.



Рисунок 2.13 – Основні недоліки у використанні цифрової ідентифікації

Стосовно ставлення до конфіденційності особистих даних при використанні цифрової ідентифікації (рисунок 2.14), виділяється кілька ключових позицій. Більшість респондентів визнають це важливим аспектом, що підкреслює

усвідомлення важливості забезпечення захисту особистої інформації під час використання цифрових ідентифікаторів. Інша частина респондентів вважає це важливим, але не завжди переживає це, що може свідчити про деяку неоднозначність або недостатню обізнаність щодо конфіденційності даних. Також є група, якій це байдуже, що вказує на можливий дефіцит усвідомлення та важливості збереження конфіденційності в цифровому середовищі. Враховуючи ці різні підходи, важливо розробляти стратегії та освітні ініціативи, спрямовані на підвищення рівня усвідомленості та важливості конфіденційності даних серед громадськості.



Рисунок 2.14 – Ставлення до конфіденційності особистих даних при використанні цифрової ідентифікації

Стосовно довіри до організацій та платформ, які зберігають особисті дані при цифровій ідентифікації (рис. 2.15), можна виділити декілька різних підходів. Зазначено, що значна кількість респондентів повністю довіряють таким організаціям, що може вказувати на впевненість у їхній здатності ефективно та безпечно зберігати особисті дані. З іншого боку, частка тих, хто не дуже довіряє чи переважно не довіряє, також є значною, що свідчить про наявність певних сумнівів та обурення стосовно захисту даних. Це визначає важливість розроблення та впровадження прозорих та надійних практик збереження особистої інформації для зміцнення довіри споживачів.



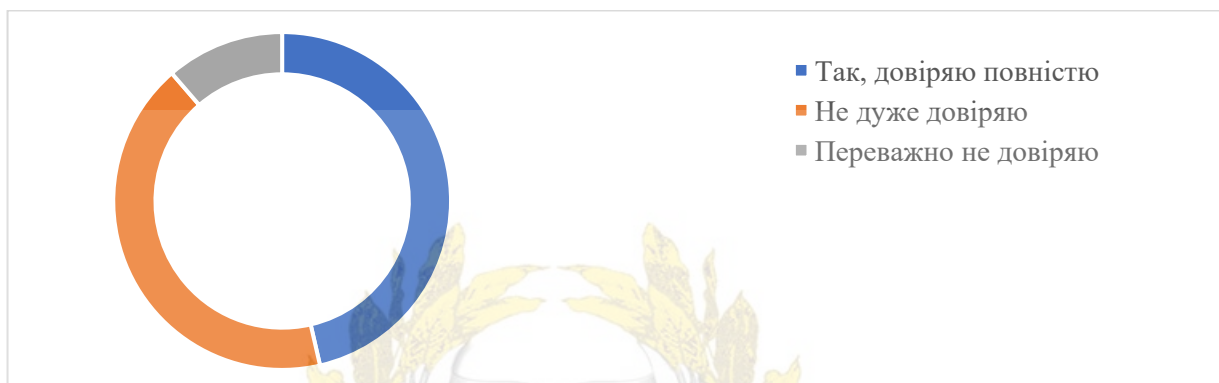


Рисунок 2.15 – Довіра організаціям та платформам, які зберігають особисті дані при цифровій ідентифікації

Розподіл рівня інформованості щодо заходів безпеки на платформах цифрової ідентифікації (рисунок 2.16) різноманітний. Деякі респонденти стверджують, що вони повністю знайомі із цими заходами. Більшість визнає, що мають деяке розуміння, але існують невідомі аспекти. Також є частина осіб, які визнали, що не володіють достатньою інформацією про заходи безпеки на платформах цифрової ідентифікації.

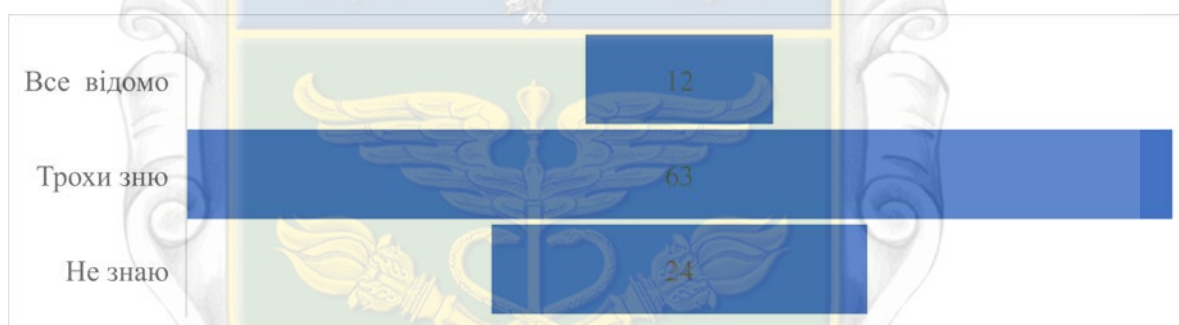


Рисунок 2.16 – Проінформованість про заходи безпеки для захисту даних на платформах цифрової ідентифікації

Щодо використання двофакторної аутентифікації (рис. 2.17) для захисту облікового запису, можна визначити різні підходи серед респондентів. Значна кількість осіб підтвердили, що вони вже використовують цей метод для підвищення безпеки свого облікового запису. Інша частина респондентів визнала, що вони знають про цей метод, але поки не використовують його. Також є невелика кількість осіб, які визнали, що не знають, як використовувати двофакторну аутентифікацію. Це може вказувати на необхідність проведення інформаційних

кампаній та навчання з метою популяризації та використання цього ефективного засобу захисту

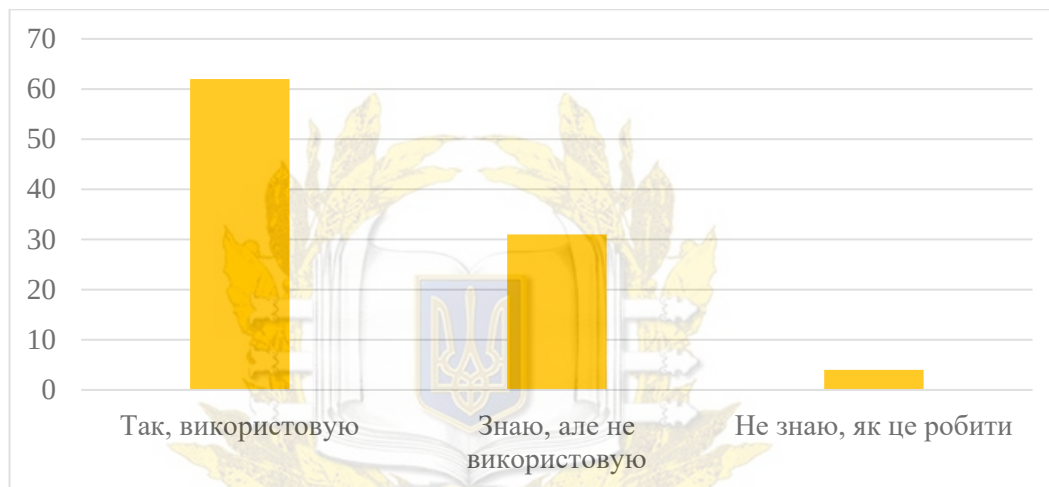


Рисунок 2.17 – Використання двофакторної аутентифікації для захисту облікового запису

Щодо відповідей на запитання на платформі цифрової ідентифікації щодо надання додаткових даних для підтвердження особистості (рис. 2.18) можна виділити різні підходи серед респондентів. Багато людей схвалюють ідею подання додаткових даних для підтвердження своєї особи на платформі. Інша частина визнала, що вагається, але в цілому готова представити відповідні дані. Також є невелика кількість осіб, які відмовилися надавати додаткові дані. Ці відповіді вказують на важливість створення прозорих та безпечних механізмів для обробки додаткових даних для підтвердження особистості на цифрових ідентифікаційних платформах.



Рисунок 2.18 – Реакція на звернення на платформі цифрової ідентифікації для надання додаткових даних для підтвердження особи

Частота змінення паролів та інших облікових даних на платформах цифрової ідентифікації може визначати рівень безпеки облікового запису користувача. Багато експертів рекомендують регулярні зміни паролів для уникнення можливих загроз безпеки. Частота змінення паролів користувачів зазначена на рис. 2.19.

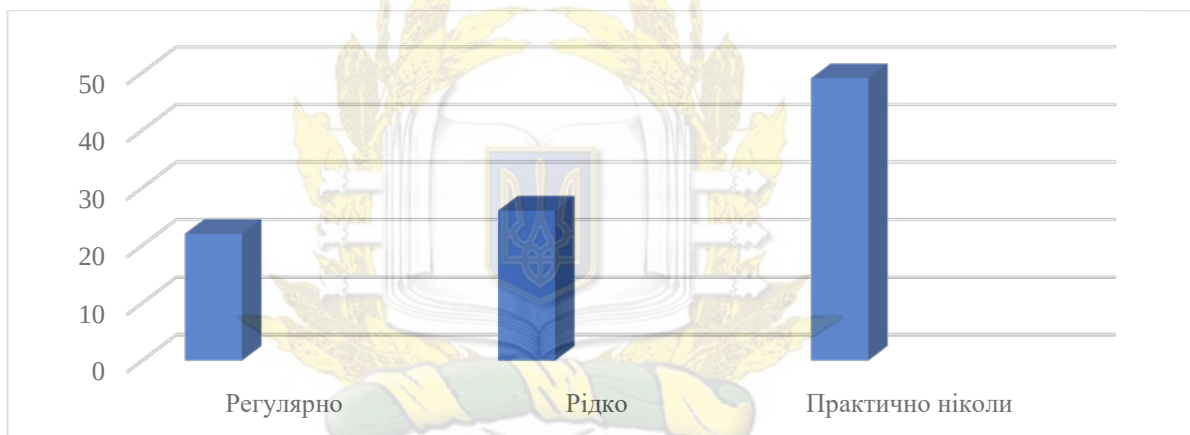


Рисунок 2.19 – Частота змінення паролів та інших облікових даних на платформах цифрової ідентифікації

Використання особистих даних без згоди користувача на платформах цифрової ідентифікації є серйозним порушенням приватності та може викликати етичні та юридичні питання. Організації та платформи повинні дотримуватися високих стандартів захисту приватності, забезпечуючи прозорі умови та можливість контролю за використанням особистих даних користувачами. В будь-якому випадку використання особистих даних без належної згоди може призвести до серйозних наслідків, включаючи порушення законодавства про захист даних та втрату довіри споживачів. Хоча більшість користувачів розуміє, що є ризик втрати даних, велика кількість вважає, що це неможливо (рис. 2.20).

Також виникає негативна реакція на повідомлення про можливий доступ третіх сторін до ваших даних на платформі цифрової ідентифікації (рис. 2.21).

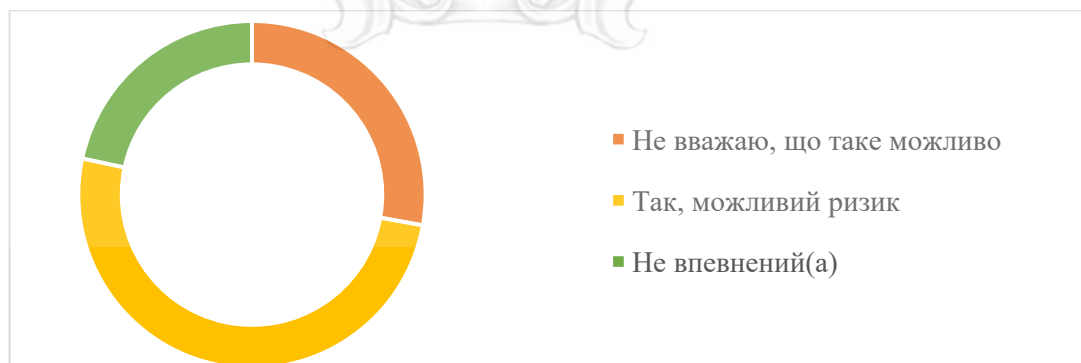




Рисунок 2.20 – Думка щодо використання особистих даних без згоди користувача на платформах цифрової ідентифікації

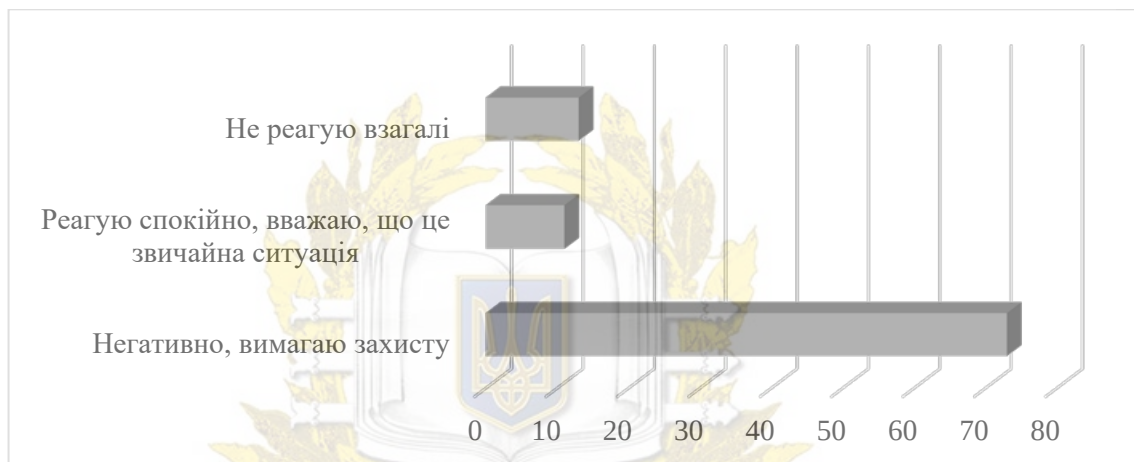


Рисунок 2.21 – Реакція на повідомлення про можливий доступ третіх сторін до ваших даних на платформі цифрової ідентифікації

Щодо знань про можливість скасування облікового запису на платформі цифрової ідентифікації при виникненні проблем можна виділити різний рівень знань серед учасників (рис. 2.22). Частина користувачів знає конкретні інструкції та процедури скасування облікового запису, в той час як інші мають загальне уявлення про можливість скасування, але не розуміють деталей цього процесу. Також є частина учасників, які не знають, як скасувати обліковий запис. Ці відповіді вказують на потребу покращення інформаційної доступності та навчання користувачів щодо процедур скасування облікових записів на цифрових ідентифікаційних платформах.

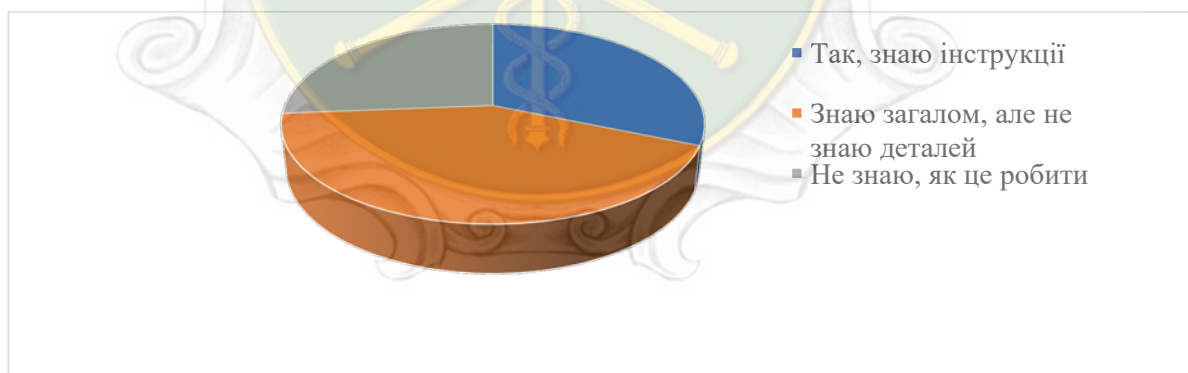


Рисунок 2.22 – Знання про скасування облікового запису на платформі цифрової ідентифікації при виникненні проблем

Згідно рис. 2.23 більшість користувачів вважає, що цифрова ідентифікація як спосіб підтвердження особи для доступу до послуг є зручною.

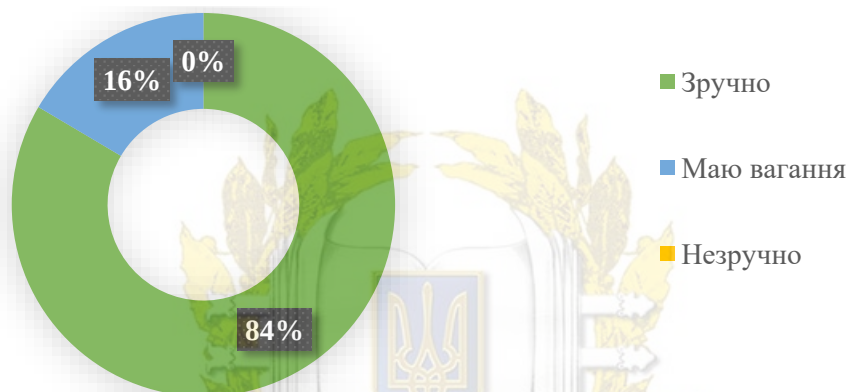


Рисунок 2.23 – Зручність цифрової ідентифікації як спосіб підтвердження особи для доступу до послуг

Щодо частоти використання цифрової ідентифікації у повсякденному житті відзначається різний рівень активності серед учасників (рис. 2.24). Більшість респондентів використовують цифрову ідентифікацію щодня, що свідчить про її широке впровадження та важливість у їхньому щоденному житті. Також є група користувачів, яка використовує це рідше, але все ще зазначає використання цифрової ідентифікації кілька разів на тиждень. Невелика кількість респондентів відзначила, що ніколи не користується цифровою ідентифікацією, що може свідчити або про відсутність необхідності, або про обмежену доступність цифрових ідентифікаційних послуг для цієї групи.

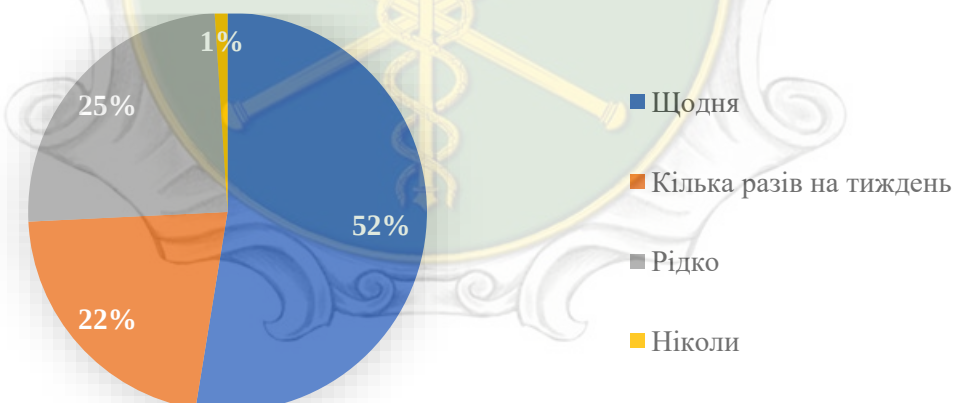


Рисунок 2.24 – Частота використання цифрової ідентифікації у повсякденному житті

Більшість користувачів вважає, що цифрова ідентифікація допомагає запобігати шахрайству та кіберзлочинам (рис. 2.25).

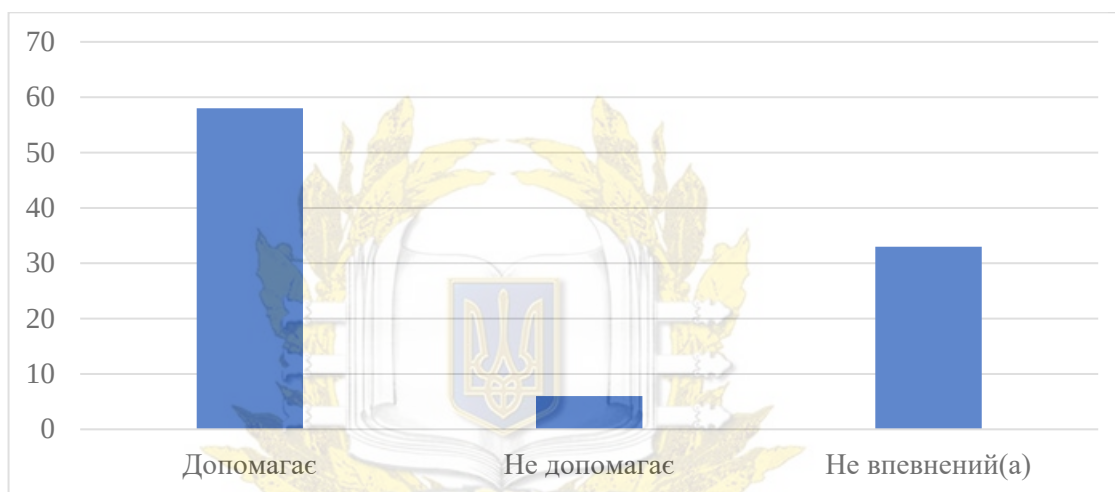


Рисунок 2.25 – Думка про допомогу цифрової ідентифікації запобігати шахрайству та кіберзлочинам

Майже всі погоджуються з тим, що цифрова ідентифікація важлива для розвитку цифрової трансформації України (рис. 2.26), тому у всіх опитуваних користувачів є в наявності смартфон з підтримкою функцій цифрової ідентифікації (рис. 2.27).

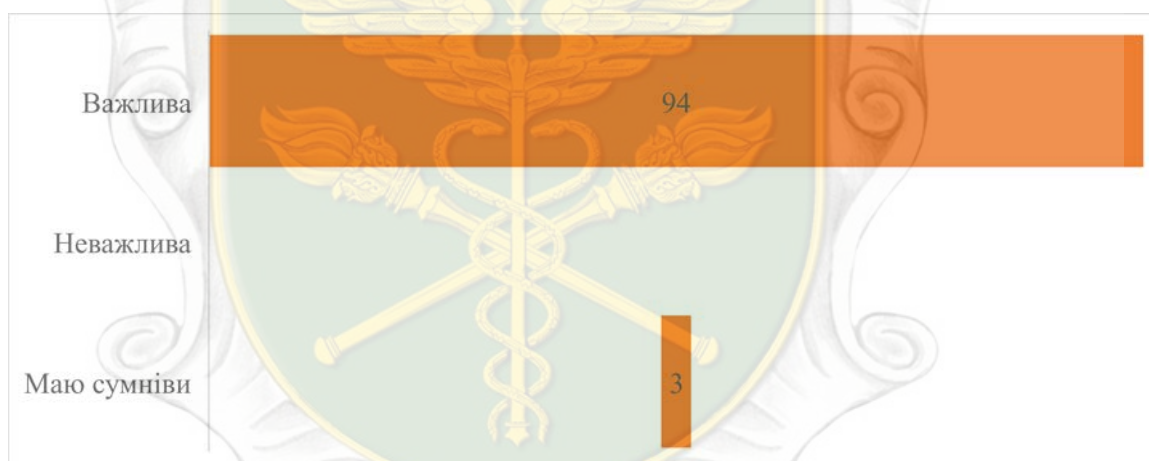


Рисунок 2.26 – Важливість цифрової ідентифікації для розвитку цифрової трансформації в Україні



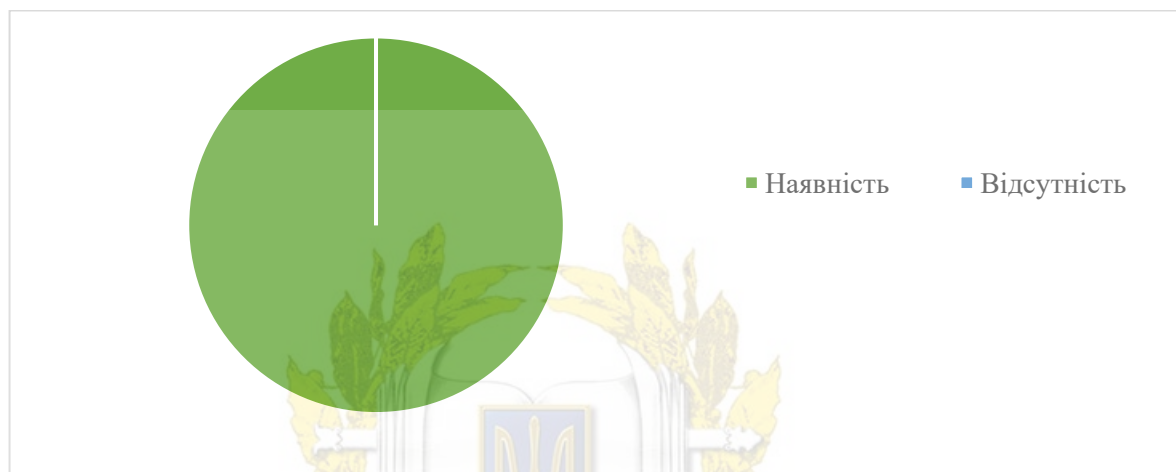


Рисунок 2.27 – Наявність смартфона з підтримкою функцій цифрової ідентифікації

Цифрова ідентифікація в Україні відіграє важливу роль у розвитку цифрової трансформації. Її важливість полягає в створенні основи для ефективної та безпечної взаємодії громадян, бізнесу та урядових органів у віртуальному просторі. Цифрова ідентифікація є ключовим елементом для забезпечення безпеки та відкритості в онлайн-середовищі, сприяє прискоренню цифрових процесів та покращенню доступу до різноманітних електронних послуг. Ця технологія сприяє вдосконаленню комунікації між різними секторами суспільства, сприяє ефективному впровадженню інновацій та підтримує загальний розвиток цифрової інфраструктури в країні. Враховуючи сучасні виклики та перспективи, цифрова ідентифікація стає ключовим фактором для досягнення цифрового прогресу та створення відкритого та динамічного цифрового середовища в Україні.

## РОЗДІЛ 3

### ВИЗНАЧЕННЯ ПРІОРИТЕТНИХ НАПРЯМКІВ УДОСКОНАЛЕННЯ СИСТЕМИ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ В ПУБЛІЧНОМУ УПРАВЛІННІ.

3.1 Забезпечення захисту конфіденційності та безпеки як пріоритетний напрямок удосконалення цифрової ідентифікації.

Згідно з експертами, основними проблемами, з якими зараз стикається цифровий розвиток України, є такі: недостатнє географічне покриття доступу до Інтернету в Україні, необхідність посилення зусиль, спрямованих на розвиток цифрових навичок у всіх сферах життя та бізнесу; відсутність офіційно затверджених стратегічних документів у сфері цифрового розвитку, а також прогалини в системі [16], немає єдиних правил для ідентифікації громадян, а також методів створення, зберігання та використання електронних даних незалежно від систем і технологій. [15]

В сучасному світі, де бізнес-структури все більше опираються на хмарні технології для зберігання та обробки даних, захист ідентифікації стає надзвичайно важливим завданням.

Застосування цифрової ідентифікації в хмарних технологіях стає обов'язковим для забезпечення безпеки та конфіденційності даних у сучасному бізнесі. Вона допомагає захистити компанійну інформацію та зберегти довіру користувачів, що є важливим аспектом успіху в цифровому світі.[51]

Розробка легкої, безпечної та доступної електронної ідентифікації є ключовою передумовою для запуску електронних послуг, електронної комерції та розвитку «цифрової» економіки.

Наступні важливі проблеми, які потрібно вирішити: збільшення кількості інформаційних систем, які використовують персональні дані; відсутність захищеного обміну ідентифікаційними даними між державними та приватними організаціями, які обробляються в інформаційних системах; неузгодженості щодо вибору ідентифікаторів; і недостатня верифікація ідентифікаційних даних. також

використання електронних механізмів ідентифікації та автентифікації, алгоритмів і протоколів, які не є технологічними, у системах реєстрації та контролю доступу до інформаційних систем.

При проходженні опитувань користувачі пропонували свої методи захисту особистих даних у цифровій ідентифікації. Найчастіше було чути про те, що їх все влаштовує. Також велика кількість користувачів знімають з себе відповідальність щодо своєї безпеки та зазначають, що над цим питанням мають працювати професіонали. Крім того, така ж кількість людей зазначає, що людям потрібно навчатись цифровій грамотності. Дані зазначені на рис. 3.1.

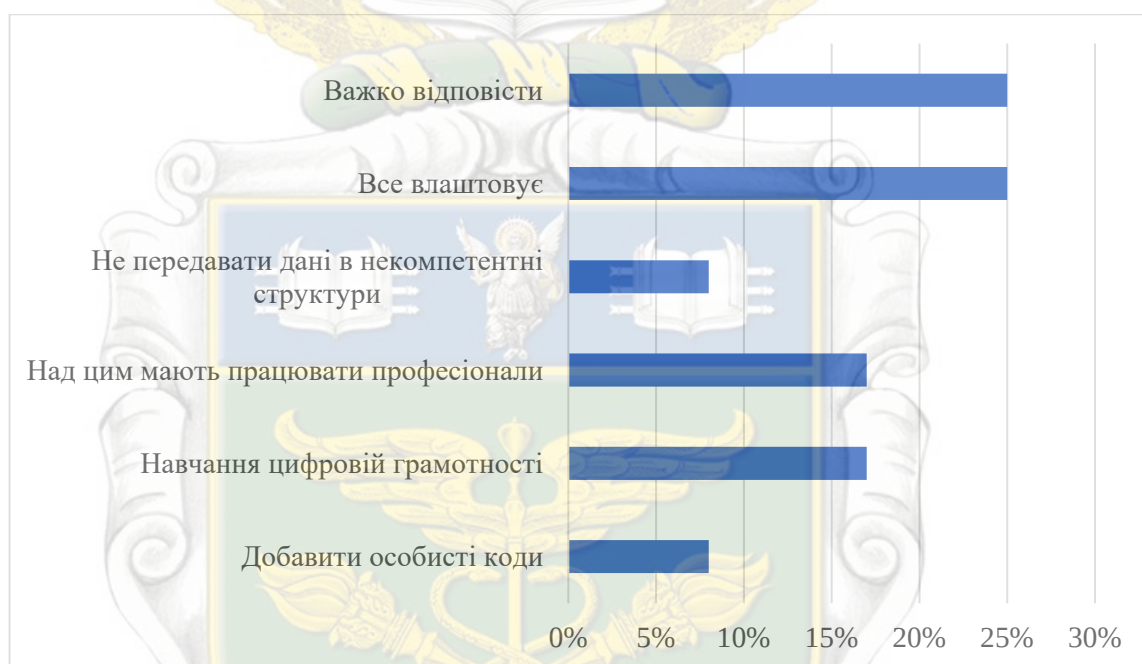


Рисунок 3.1 – Запропоновані заходи захисту особистих даних у цифровій ідентифікації

Підвищення надійності цифрової ідентифікації стане основою «цифрових» операцій, оскільки державні організації та громадяни використовуватимуть усе більше цифрових технологій. Державні організації використовують комплекс процесів і технологій, відомих як електронна ідентифікація громадян (e-ID), щоб створити безпечну середовище, де люди можуть отримати доступ до основних ресурсів або послуг. Оскільки методи особистої перевірки вже надто застарілі для надання громадянам комплексного та безперешкодного доступу до ресурсів і послуг, державні організації повинні вимагати авторизацію та підтвердження



особи, що виконується в Інтернеті. У рамках цієї бізнес-моделі «єдиного вікна» необхідно забезпечити можливість надання кожному жителю унікального, постійного ідентифікатора, який відповідає культурним і правовим стандартам. [45]

У ситуаціях війни безпека особистих даних у цифровій ідентифікації стає надзвичайно важливою, оскільки конфіденційність та захист інформації стають ключовими аспектами в умовах загроз та ворожого впливу. У цьому контексті важливо посилити технічні засоби шифрування та гарантувати захист особистих даних від несанкціонованого доступу та кібератак. Також доцільно розглядати можливість використання анонімізації та псевдонімізації для збереження ідентифікаційних даних під час обробки та передачі інформації.

Ситуації війни також вимагають розробки та впровадження стратегій контролю доступу, щоб гарантувати, що особисті дані використовуються лише з необхідною метою та за належними повноваженнями. Значущим є і вдосконалення заходів моніторингу та виявлення можливих кіберзагроз, спрямованих на порушення безпеки особистих даних у воєнний період. Ефективні системи виявлення інцидентів та їх негайного вирішення можуть виявляти та ліквідовувати потенційні загрози, забезпечуючи захист особистих даних під час воєнних дій.

Постановою, від 17 березня 2022 р., Кабінет Міністрів України установив, що:

1. У період воєнного стану на території України та протягом місяця з дня його припинення чи скасування кваліфіковані надавачі електронних довірчих послуг можуть автоматично створювати нові сертифікати раніше засвідчених відкритих ключів для користувачів електронних довірчих послуг без особистої присутності користувачів.

Старий сертифікат скасовується, а новий сертифікат користувача електронних довірчих послуг не може мати більше трьох років. Крім того, строк дії нового користувача електронних довірчих послуг не може перевищувати строк дії кваліфікованого сертифіката відкритого ключа надавача електронних довірчих послуг.

2. Під час введення воєнного стану в Україні та протягом шести місяців після його припинення або скасування дозволяється використовувати електронні підписи та печатки, які базуються на сертифікатах відкритого ключа, виданих кваліфікованими надавачами електронних довірчих послуг. Кваліфіковані системи електронного підпису та печатки не повинні зберігати інформацію про особистий ключ. Користувачі електронних довірчих послуг можуть використовувати це для електронної взаємодії, електронної ідентифікації та автентифікації фізичних осіб, юридичних осіб і їх представників. Цей потенціал, однак, обмежений, якщо законодавство вимагає використання виключно кваліфікованих електронних підписів та печаток або якщо висока інформаційна безпека вимагає використання засобів електронної ідентифікації з високим рівнем довіри.

3. В період воєнного стану на території України та протягом шести місяців з дня припинення чи скасування воєнного стану кваліфікований надавач електронних довірчих послуг, державне підприємство «ДІА», надає послугу з формування кваліфікованого сертифіката відкритого ключа, який дозволяє створювати, перевіряти та підтверджувати віддалений кваліфікований електронний підпис «Дія.Підпис» або «Дія ID» доступний безкоштовно.

Мобільний додаток Єдиного державного веб-порталу електронних послуг (Дія) дозволяє особам, які отримали паспорт громадянина України, посвідку на постійне проживання, посвідку на тимчасове проживання або паспорт громадянина України для виїзду за кордон, або будь-яку іншу форму посвідки, оформлену за допомогою Єдиного державного демографічного реєстру, за власним бажанням отримати ці послуги за умови їх дійсності, використовується для дистанційного ідентифікації цих осіб без їх особистої присутності в офісі кваліфікованого надавача електронних довірчих послуг або в його відокремленому пункті реєстрації:

1) ідентифікувати особу за допомогою інформації Єдиного державного демографічного реєстру, яку можна знайти за допомогою запиту, отриманого за допомогою єдиної інформаційної системи МВС на мобільному додатку Дія. Портал Дія містить інформацію, яка дозволяє однозначно ідентифікувати особу.

Підготовка запиту ґрунтується на ідентифікаційних даних особи, отриманих за допомогою системи BankID Національного банку або отриманих особою за допомогою мобільного додатка Порталу Дія (Дія) за допомогою безконтактного електронного носія, імплантованого в паспорт громадянина України, паспорт громадянина України для виїзду за кордон, посвідку на постійне проживання або посвідку на тимчасове проживання;

2) перевірка того, чи дійсні видані особі паспорти громадянина України, паспорти громадянина України для виїзду за кордон, посвідки на постійне проживання, посвідки на тимчасове проживання, які були створені за допомогою Єдиного державного демографічного реєстру, використовуючи інформацію, отриману з Єдиного державного демографічного реєстру, а також бази даних про викрадені (втрачені) документи за зверненнями громадян у Єдиній інформаційній системі;

3) розпізнавання обличчя за допомогою порівняння фотозображення особи, створеного за допомогою мобільного додатка Порталу Дія (Дія), з відцифрованим зображенням особи, переданим з Єдиного державного демографічного реєстру за допомогою єдиної інформаційної системи МВС до мобільного додатка Порталу Дія (Дія), або читання;

4) впровадження додаткових процедур підтвердження особи відповідно до регламенту роботи кваліфікованого надавача електронних довірчих послуг «ДІА». [11]

Але, штучне стимулювання цифровізації може призвести до певних ризиків, особливо коли йдеться про системи біометричної ідентифікації з імплантацією. Хоча такі технології мають потенціал поліпшити безпеку та зручність, їх впровадження повинно супроводжуватися обов'язковими заходами та обережністю. [49]

Аналізуючи опитування, що зазначені у другому розділі, ми дійшли висновку, що більшість людей не розуміє небезпеки, яку несе в собі збір персональних даних. Вже зараз на основі цього великі компанії впливають на вибір та підсвідомість величезних груп людей. Треба вводити у шкільну програму



предмет, на якому мають розповідати яким чином збирають інформацію про особистість, розглядати детально угоди програмного забезпечення і приносити у свідомість людини відповідальність за дії, які вона робить в цифрових мережах.

Також, потрібно грамотно інформувати старше покоління про цифрову ідентифікацію та небезпеку збору інформації.

Багато учасників говорили про те, що потрібно використовувати технологію блокчейн.

Блокчейн — це технологія, яка дозволяє створювати надійні та безпечні записи або «блоки» та об'єднувати їх у ланцюжок, де інформація про кожен новий блок міститься в попередньому. Основна перевага полягає в тому, що ця інформація захищена від втрати та модифікації. Блокчейн використовується для створення безпечних електронних записів, які можна використовувати в багатьох сферах, таких як фінанси, логістика та медицина, серед інших. Завдяки цій технології учасники можуть створювати довіру, не вдаючись до посередників, і інформація може бути перевірена на надійність.

Однією з можливих розробок у сфері захисту конфіденційності та безпеки цифрової ідентифікації може бути створення інноваційного інтегрованого рішення для керування та захисту особистих даних.

Ця розробка представляла б собою новаторську систему цифрової ідентифікації, яка базується на технології блокчейн. Ця система надавала б користувачам вищий рівень безпеки, контролю та прозорості в управлінні їх особистими даними. Унікальний цифровий ідентифікатор, який кожен користувач отримує, зберігається в блокчейні, забезпечуючи децентралізований підхід до ідентифікації.

Основна перевага полягає в використанні технології блокчейн для ефективного захисту особистих даних шляхом шифрування та розподіленого зберігання. Застосування смарт-контрактів дозволяє автоматизувати та перевіряти ідентифікаційні процеси для забезпечення точності та достовірності інформації. Користувачі мають повний контроль над своєю інформацією та можуть встановлювати права доступу для інших сторін.

Додатковий рівень аутентифікації досягається за рахунок використання біометричних даних, які криптографічно захищені в блокчейні. Щоб забезпечити анонімність та конфіденційність, система використовує анонімні транзакції.

Таким чином система забезпечить високий рівень безпеки особистих даних, використовуючи технологію блокчейн для ефективного захисту інформації. Використання смарт-контрактів дозволить автоматизувати та перевіряти процеси ідентифікації, забезпечуючи точність та достовірність даних. Користувачі матимуть повний контроль над своєю інформацією та можливість встановлювати права доступу.

Застосування біометричних даних та анонімних транзакцій у блокчейні покращить безпеку та конфіденційність. Очікується, що вона стане високоефективною альтернативою традиційним методам цифрової ідентифікації, використовуючи інноваційні підходи до захисту особистих даних та відкриваючи нові можливості в застосуванні технології блокчейн.

### 3.2 Забезпечення доступності, інтеграції та співпраці в контексті удосконалення цифрової ідентифікації.

Регламент № 910 (eIDAS) був прийнятий у 2014 році ЄС з метою встановлення єдиних стандартів для розвитку електронної ідентифікації, а також для надання електронних довірчих послуг у країнах ЄС, а також для розвитку електронної ідентифікації між країнами ЄС.

З іншого боку, метою Secure idenTity acrOss boRders linKed 2.0 (Stork 2.0) є створення єдиного середовища для електронної ідентифікації та автентифікації в ЄС. Основним напрямком проекту є розробка стандартів, форматів, ідентифікаторів тощо для впровадження інтероперабельних засобів електронної ідентифікації, таких як е-медицина, електронні публічні послуги та е-банкінг.

Проект також повинен сприяти розвитку цифрового єдиного ринку ЄС, запровадженню транскордонної взаємодії та збільшенню мобільності громадян і компаній ЄС. Приєднання до цих проектів сприятиме розвитку е-ідентифікації, яка відповідає вимогам ЄС і допоможе Україні євроінтегруватися. [45]

Згідно з аналізом документів для досягнення KPI необхідно було створити інфраструктуру ідентифікації та довіри, таку як citizen ID, mobile ID та bank ID, з метою забезпечення цифрової ідентифікації для 99,9% громадян до 2020 року. Загальна потреба в інвестиціях на протязі 10 років складає 300 мільйонів доларів.

На основі вітчизняного та зарубіжного досвіду розробка та впровадження сучасних інформаційно-комунікаційних технологій в системі публічного управління в Україні пов'язана з необхідністю підвищення рівня інформаційної активності державних службовців та громадян шляхом використання різноманітних інформаційних контентів, які мають науковий, технічний, соціально-економічний, правовий та громадський характер, щоб вирішити поточні соціально-економічні проблеми країни. [27]

Стратегічний вектор розвитку України – інтеграція в Європейський центральний банк, пріоритети співпраці між Україною та ЄС, оскільки це необхідно для забезпечення економічної безпеки, конкурентоспроможності та соціально-економічного прогресу [1], договори щодо підтримки ЄС електронного урядування та цифрової економіки в Україні [2], активну діджиталізацію у ЄС, на сучасному етапі розвитку України дослідження стану, особливостей та результатів діджиталізації країн ЄС становить значний науковий та практичний інтерес. [22]

Розвиток інституційного забезпечення цифрових трансформацій у ЄС визначається низкою ключових стратегічних документів, включаючи:

1. Цифрова стратегія Європейської Комісії: Перетворення Комісії в цифровоорієнтовану, спрямовану на користувачів та оптимізовану на основі даних.
2. Стратегія єдиного цифрового ринку для Європи: Створення єдиного цифрового ринку в Європі.
3. Формування цифрового майбутнього Європи: Розвиток стратегії для цифрового майбутнього.



4. Біла книга з штучного інтелекту. Європейський підхід до досконалості і довіри: Визначення європейського підходу до розвитку штучного інтелекту.
5. Європейська стратегія щодо даних: Розробка стратегії для роботи з даними.
6. План дій Європейської Комісії щодо 5G: Визначення заходів для розвитку мереж 5G.
7. Директива про безпеку мереж та інформаційних систем: Регулювання питань безпеки мереж та інформаційних систем.
8. План дій з цифрової освіти: Розвиток стратегії щодо цифрової освіти.
9. Стратегія взаємодії урядів ЄС: Визначення стратегії для покращення взаємодії між урядами ЄС.
10. Цифровий компас 2030: Європейська стратегія для цифрового десятиліття у 2030 році. [22]

Цифровий компас 2030 (2030 Digital Compass: the European way for the Digital Decade): європейський шлях цифрового десятиліття є одним із найважливіших стратегічних документів ЄС, який визначає цифрові трансформації як основу розвитку ЄС до 2030 року. [25]. Згідно з цим стратегічним документом, цифрові трансформації в ЄС мають бути зосереджені на таких пріоритетних напрямках до 2030 року:

- 1) розвиток цифрових навичок і підготовка висококваліфікованих працівників в галузі цифрових технологій. кваліфіковані люди та висококваліфіковані цифрові техніки. До 2030 року щонайменше 80% дорослих повинні мати базові навички роботи з цифровими технологіями, а в ЄС має бути зайнятих 20 мільйонів спеціалістів у сфері інформаційних та комунікаційних технологій; створювати та підтримувати стійкі, безпечні та ефективні цифрові інфраструктури. До 2030 року Європа повинна мати свій перший квантовий комп'ютер; всі населені райони повинні мати гігабітне з'єднання, а виробництво передових і стійких напівпровідників у Європі має становити 20% світового виробництва; 10 000 кліматично нейтральних високо безпечних крайніх вузлів мають бути розгорнуті в ЄС. Створити умови та гарантувати цифрову

трансформацію бізнесу. До 2030 року кількість компаній-єдинорогів ЄС повинна подвоїтися, а кількість послуг хмарних обчислень, великих даних і штучного інтелекту повинна бути вдвічі збільшена; більше 90% малих та середніх підприємств повинні досягти принаймні базового рівня цифрової інтенсивності; і три з чотирьох компаній повинні використовувати послуги хмарних обчислень, штучного інтелекту та штучного інтелекту. До 2030 року кожен громадянин матиме можливість отримати електронну пошту. Всі основні державні послуги будуть доступні в Інтернеті [22].

Вкрай важливо розуміти, що основною метою цих реформ є систематизація даних, а не впровадження інформаційних технологій. Це дозволить якісно обробляти, зберігати, захищати та аналізувати дані. Крім того, необхідно підвищити рівень освіти в галузі інформаційних технологій і покращити навички використання Інтернету як державними діячами, так і широким загалом[36].

Таким чином, наведено 10 основних стратегічних технологій, які, мають вирішальне значення для державного сектору України:

1) «Цифрове» робоче місце. Від рядових працівників до керівників вищої ланки державні установи все частіше наймають працівників, які мають навички роботи з цифровими технологіями. «Цифрове» робоче місце — це стратегія бізнесу, яка дозволяє працівникам бути більш мобільними та ефективними в організації. «Цифрове» робоче місце дозволяє співробітникам спільно працювати та взаємодіяти, підтримувати децентралізовані та мобільні робочі місця та дозволити їм особисто вибирати технології. Зниження витрат на апаратне забезпечення, відрядження та офісні приміщення є одними з переваг «цифрових» робочих місць. Крім того, «цифрові» робочі місця більш конкурентоспроможні при пошуку працівників, оскільки вони пропонують сучасну, інноваційну корпоративну культуру, кращий баланс між особистим життям і роботою, а також соціальний стиль роботи, який подобається розумним поколінням міленіалів. Натомість державні службовці повинні виконувати більш захоплюючі та інноваційні завдання.

2) Багатоканальне залучення громадян і інформація для того, щоб взаємодіяти з людьми, необхідно використовувати комплексний підхід, який охоплює всі канали. Цифрові технології перетворюють макрорівень «громадян» на мікрорівень «конкретного громадянина», а діяльність «інформування» перетворюється на «залучення». Державні установи потребують нових способів виявлення та розуміння потреб і бажань громадян. Це включає використання соціальних мереж і комунікацій для активного залучення до політичних процесів, надання громадянам можливостей долучитися на їхніх власних умовах, надання їм можливості бути персоналізованими, і багато іншого. Вкрай важливо використовувати стратегію управління інформацією та зворотній зв'язок громадян, яка передбачає можливості багатоканального залучення та інформування, щоб забезпечити комунікацію, пояснення та швидку адаптацію. Це особливо важливо під час реформ.

3) Підвищення надійності цифрової ідентифікації стане основою «цифрових» операцій, оскільки державні організації та громадяни використовуватимуть усе більше цифрових технологій. Державні організації використовують комплекс процесів і технологій, відомих як електронна ідентифікація громадян (e-ID), щоб створити безпечну середовище, де люди можуть отримати доступ до основних ресурсів або послуг. Оскільки методи особистої перевірки вже надто застарілі для надання громадянам комплексного та безперешкодного доступу до ресурсів і послуг, державні організації повинні вимагати авторизацію та підтвердження особи, що виконується в Інтернеті. У рамках цієї бізнес-моделі «єдиного вікна» необхідно забезпечити можливість надання кожному жителю унікального, постійного ідентифікатора, який відповідає культурним і правовим стандартам.

4) Відкриті дані означають, що певні дані можуть бути вільними для використання та розповсюдження будь-яким, за умови дотримання правил атрибуції та (або) ліцензії на спільне використання. Розвиток інформаційних технологій та інтернету призвів до активного поширення ідеї. Одним із різновидів відкритих даних є відкриті державні дані, які служать інструментом для оцінки та моніторингу діяльності державних і політичних органів. Відкриті дані



публікуються як у вигляді даних із визначеними налаштуваннями конфіденційності, безпеки або якості, так і у вигляді неопрацьованих даних із джерела з найнижчим рівнем деталізації. Торгові марки та авторські права не обмежують доступ до відкритих даних у програмних інтерфейсах застосунків.

5) Повсюдна аналітика — це постійний, динамічний процес збору та аналізу інформації (знань) з даних з метою отримання актуальної та структурованої інформації (знань) для ситуаційної та стратегічної діяльності, а також для створення планів дій, програм, ініціатив і ініціатив. Використання аналітики на всіх етапах урядової та державної діяльності та надання послуг, або повсюдна аналітика, дозволяє державним установам перейти від стандартизованої аналітичної звітності із запізнілими даними до автономних бізнес-процесів, а також можливостей бізнес-аналітики, які можуть приймати кращі рішення в режимі реального часу на основі актуальних і всеохоплюючих даних.

6) «Інтернет речей» — це мережа фізичних об'єктів (фіксованих або мобільних) з технологіями для обміну інформацією, спостереження, сенсорної взаємодії та інших функцій. Архітектура «інтернету речей» є одним із найважливіших елементів для функціонування цифрових бізнес-застосунків у всіх галузях приватного та державного секторів економіки. Він функціонує в екосистемі, до якої входять фізичні об'єкти (речі), засоби зв'язку, застосунки та аналіз даних. Сфера послуг або завдань визначає кількість прикладів використання «інтернету речей» і швидкість його впровадження державними установами. Наразі державні установи починають використовувати «інтернет речей» для своєї діяльності. Прикладами таких моделей є «оплата за використання» або моделі оподаткування за передплатою, «розумний» збір сміття на міських вулицях, віддалений моніторинг старих людей у будинках престарілих, моніторинг екології та багато іншого.

7) Фактично «розумні» машини та засоби складаються з різноманітних цифрових технологій, які мають здатність виконувати завдання, на які раніше була здатна лише людина. Зараз доступні глибокі нейронні мережі, автономні транспортні засоби, віртуальні помічники, «розумні» радники та «віртуальні»

секретарі, які інтелектуально взаємодіють з іншими машинами та людьми. Створення нових послуг і вдосконалення існуючих методів діяльності державних установ можна досягти за допомогою «розумних» інструментів і систем. Нові послуги включають такі речі, як системи автоматичного оперативного оповіщення щодо надзвичайних ситуацій, голосові послуги державних контакт-центрів і різноманітні інтелектуальні застосування, які полегшують взаємодію бюрократії з державними установами.

8) «Цифрові» платформи, створені урядом. Сучасні державні установи намагаються одночасно збільшити якість послуг, скоротити кількість працівників і зменшити витрати. «Цифрові» платформи, такі як системи ERP і CRM, можуть вирішувати ці проблеми, значно збільшуючи ефективність, зменшуючи вартість діяльності та час виконання. Державні установи використовують «цифрові» платформи для скорочення витрат, покращення взаємодії з громадянами та спрощення внутрішніх процесів.

9) Програмно-конфігуровані архітектури – необхідно «вдихнути нове життя» старим технологіям, тому віртуалізація мереж, інфраструктур і систем безпеки є корисним способом масштабування та використання ІКТ-систем. Відповідне програмне забезпечення дозволяє швидко створювати та запускати нові більш складні архітектури. Це дозволяє державним органам швидко розробляти проекти в галузі «електронного» урядування, «інтернету речей» і т. д. без додаткових витрат.

10) Блокчейн є потужним інструментом, який може змінити політику держави в таких областях, як нотаріат, біржа, правосуддя та ідентифікація особи. Блокчейн — це технологія, яка використовується в розподіленій одноранговій мережі загального користування, яка має здатність зберігати інформацію про правочини, або транзакції, на постійній основі без можливості змінювати її. Крім того, криптографічні інструменти захищають мережу. Електронні референдуми, е-петиції, е-голосування та електронне урядування є кількома можливостями, доступними через мережі блокчейн, особливо щодо сфери державного управління. Блокчейн дозволяє створювати повністю децентралізовані системи та забезпечує

надзвичайно високий рівень захисту даних. Система може бути використана в таких важливих областях, як електронні фінанси, державні закупівлі та електронні бюджети, оскільки вона захищена від атак. Через те, що Україна є домом для чверті світових блокчейн-проектів, країна ідеальна для проведення досліджень і розробок у цій технології, а державний сектор є найкращим майданчиком для таких проектів. Зазначені десять стратегічних технологій можуть перетворити державний сектор України, який складається з таких секторів, як освіта, медицина, транспорт, обслуговування тощо, на «центр апробації, використання та розвитку технологій», який матиме глобальний вплив протягом наступних п'ятнадцяти-двадцяти років. Вони, безсумнівно, створять нові проблеми та виклики для громадян, державних чиновників, експертів і професійних спільнот.

Зважаючи на глобальну пандемію COVID-19, виникла необхідність у зміні багатьох аспектів нашого життя, включаючи спосіб, яким ми отримуємо доступ до господарських та соціальних послуг. Всесвітня криза вимагала швидких та інноваційних рішень для підтримки громадян та підтримки нормального функціонування суспільства.

В цьому контексті платформа "Дія" стала ключовим інструментом для надання послуг та вирішення різноманітних адміністративних питань в Україні. За час пандемії, використання цієї платформи значно зросло, а разом з ним і важливість цифрової ідентифікації стала надзвичайно актуальною.

Цифрова ідентифікація через платформу "Дія" дозволила користувачам підтверджувати свою особистість онлайн, що важливо в умовах обмежень та соціального дистанціювання. Вона стала важливим інструментом для забезпечення безпеки та зручності при використанні громадських служб та ресурсів, що вимагають особистого відвідування раніше. Ця зміна використання платформи "Дія" та підвищений попит на цифрову ідентифікацію свідчать про необхідність і актуальність цифрових інструментів у подібних кризових ситуаціях, а також розвиток онлайн-сервісів для зручності та безпеки громадян.[50]

В останні кілька років у владному, науковому та експертному середовищі наголошувалося на розробці концепції цифрової економіки та цифрової



трансформації локальних територій України. Крім того, вкрай важливо створити теоретико-методичні основи для оцінки ефективності та результативності конкретних заходів. В умовах воєнного стану ця потреба посилюється завдяки широкому розповсюдженню та використанню різних цифрових інструментів, які охоплюють всі сфери життєдіяльності регіону та територіальної громади. Цифровізація сприяє розвитку територій України, постраждалих від війни, надаючи адміністративні, соціальні, економічні та інші послуги на місцях. Команда Міністерства цифрової трансформації України планувала створити індекс цифрової трансформації регіонів наприкінці 2021 року, але активні воєнні дії змусили цей план втілитися лише в березні 2023 року.

Одним із інструментів для вимірювання процесів інформатизації та цифровізації в 24 регіонах України є Індекс цифрової трансформації регіонів, який дозволяє дослідити спроможність органів влади приймати цифрові рішення та визначити рівень цифрової культури серед громадян нашої держави. Загалом Індекс цифрової трансформації регіонів України складається з восьми підіндексів, у яких представлено 31 індикатор і 76 показників [28]. Результати розрахунку індексу цифрової трансформації регіонів та значень його субіндексів демонструє додаток Г.

Удосконалення системи цифрової ідентифікації в публічному управлінні полягає в тому, щоб зробити її простою для всіх користувачів. Це означає, що система повинна бути доступною для людей з візуальними, слуховими, фізичними або когнітивними обмеженнями. Для цього важливо враховувати їхні можливості та потреби під час розробки системи.

Можливість використовувати адаптивні технології та інші інструменти, які полегшують доступ до системи для людей з обмеженими можливостями, є важливим елементом доступності. Крім того, система повинна підтримувати кілька мов і дозволяти користувачам, які належать до різних мовних груп і культур, перекладати інтерфейс.

Багато людей використовують мобільні пристрої для отримання інформації та послуг, що робить мобільний доступ важливим, особливо під час пандемії.

Доступ до системи через мобільні пристрої покращує зручність користувачів. Крім того, необхідно забезпечити, щоб система була доступною для користувачів, які проживають у віддалених районах, де може бути обмежений доступ до Інтернету. Це може включати можливість використовувати систему офлайн або через повільне з'єднання Інтернету.

Загалом, успіх і використання системи цифрової ідентифікації громадянами з різними потребами та можливостями залежить від забезпечення доступності.

Поєднання в системі цифрової ідентифікації в публічному управлінні визначається як один з ключових аспектів, на який слід звернути увагу. Потрібно забезпечити безперешкодний обмін даними та інформацією між різними електронними платформами та сервісами. Важливо, щоб система цифрової ідентифікації була вбудована в єдину інформаційну інфраструктуру, яка об'єднує різноманітні електронні сервіси, спрощуючи використання різних послуг громадянами без постійної необхідності повторної ідентифікації.

Крім того, інтеграція системи з іншими урядовими органами стає важливим елементом для полегшення взаємодії громадян із державними службами та оптимізації надання послуг. Також система повинна безперешкодно взаємодіяти з електронними ресурсами, такими як бази даних та системи електронного документообігу, використовуючи їх для публічного управління.

Інтеграція повинна відбуватися таким чином, щоб користувачі легко користувалися різними послугами, не замарюючись складними процесами ідентифікації чи взаємодії з різними платформами. Під час цього процесу також необхідно забезпечити високий рівень безпеки даних та конфіденційності, щоб інформація користувачів залишалася захищеною під час обміну даними між різними системами. Інтеграція визначає необхідність створення єдиної електронної інфраструктури, яка спрощує взаємодію громадян з державними службами та забезпечує доступ до послуг без додаткових труднощів.

У сфері публічного управління необхідно активно співпрацювати з різними стейкхолдерами, щоб удосконалити систему цифрової ідентифікації. Для

досягнення ефективності та успішності системи урядові органи, громадськість і міжнародні партнери взаємодіють.

Партнерство з громадськістю виявляється важливим, оскільки співпраця з громадськими організаціями дозволяє враховувати бажання та потреби громадян щодо цифрової ідентифікації. Ключовим кроком до покращення системи є врахування думок громадян.

Урядова співпраця — це робота різних урядових органів разом, щоб створити та підтримувати систему цифрової ідентифікації. Це охоплює обмін інформацією та ресурсами для створення єдиної інфраструктури.

Оскільки існують глобальні стандарти та передові практики в галузі цифрової ідентифікації, міжнародна співпраця є життєво важливою. Співпраця з іншими країнами та міжнародними організаціями сприяє впровадженню найкращих практик та стандартів у систему.

Співпраця з організаціями, які відповідають за захист приватності та інформації громадян, називається захистом даних. Спільні заходи зменшують ймовірність витоку даних.

Для того, щоб навчити користувачів і працівників урядових органів щодо переваг та безпеки цифрової ідентифікації, освіта та навчання виявляються важливим компонентом співпраці з освітніми установами.

Успішне впровадження та функціонування системи цифрової ідентифікації вимагає співпраці. Це дозволяє залучати різні стейкхолдерів та забезпечити оптимальний розвиток системи, який допомагає громадянам і загальному суспільству.



## ВИСНОВКИ ТА ПРОПОЗИЦІЇ

В ході проведеного дослідження мету було досягнуто, завдання виконано, а отримані результати дозволяють зробити наступні висновки.

1. Сфера електронної ідентифікації є основою для встановлення довіри між учасниками економічних операцій і учасниками електронних послуг. У «цифровій» економіці вважається, що встановлення довіри є життєво важливим для успішного функціонування. Розширення використання електронних транзакцій значною мірою обмежується організаційними, правовими та технологічними проблемами довіри. Це означає, що населення продовжує функціонувати в традиційних фізичних формах соціально-економічної взаємодії. Таким чином, роль державної політики України в галузі електронної ідентифікації є вирішальною. Для створення довіри та розвитку «цифрової» економіки важливо створити надійну та безпечну інфраструктуру та впровадити міжнародні стандарти.

2. Різноманітні стратегії і ініціативи, які можуть допомогти вдосконалити системи цифрової ідентифікації, надають широкі можливості для подальшого розвитку цього процесу. Наше бачення полягає в різних аспектах використання біометричних даних, таких як відбитки пальців або сканери обличчя, може значно підвищити точність ідентифікації особи та запобігти можливим випадкам шахрайства.

3. Впровадження технологій блокчейн може забезпечити надійність і безпеку системи цифрової ідентифікації, а також дозволити громадянам мати більший контроль над своїми особистими даними. Також, мультифакторна аутентифікація є необхідною для підвищення рівня безпеки, і важливо використовувати кілька різних методів аутентифікації, таких як біометричні дані, паролі та підтвердження через смартфон.

4. Підвищення рівня обізнаності серед населення щодо правил та безпеки використання цифрової ідентифікації може бути досягнуто через організацію кампаній та освітніх програм.

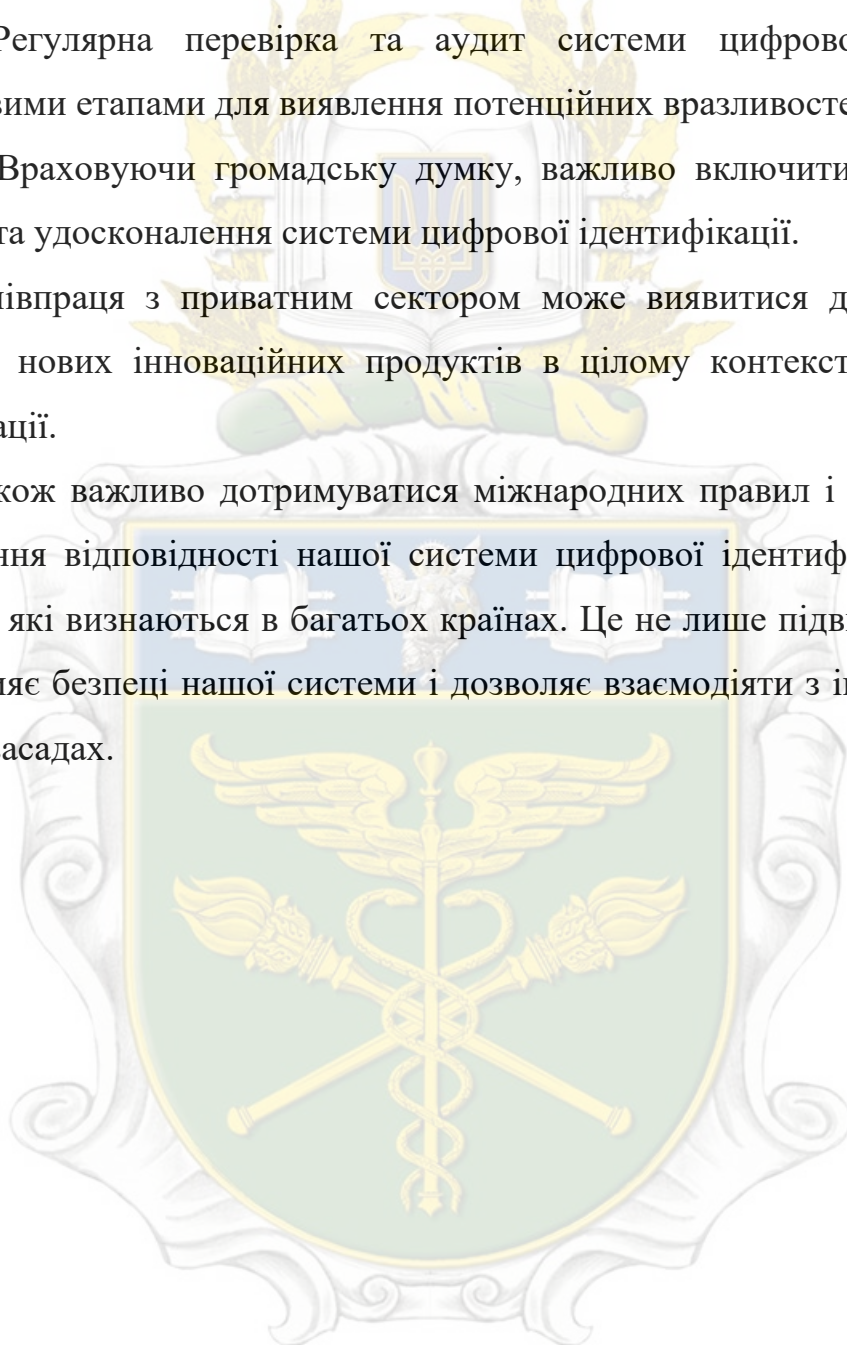
5. Щоб забезпечити ефективну взаємодію та сумісність різних систем цифрової ідентифікації, важливо розробити стандарти та відповідність, а захист особистих даних та конфіденційності є ключовим завданням і повинен ефективно забезпечувати безпеку громадянських даних від несанкціонованого доступу.

6. Регулярна перевірка та аудит системи цифрової ідентифікації є обов'язковими етапами для виявлення потенційних вразливостей та помилок.

7. Враховуючи громадську думку, важливо включити публіку в процес розробки та удосконалення системи цифрової ідентифікації.

8. Співпраця з приватним сектором може виявитися дієвим засобом для створення нових інноваційних продуктів в цілому контексті систем цифрової ідентифікації.

9. Також важливо дотримуватися міжнародних правил і стандартів як засіб забезпечення відповідності нашої системи цифрової ідентифікації стандартам і правилам, які визнаються в багатьох країнах. Це не лише підвищує ефективність, але й сприяє безпеці нашої системи і дозволяє взаємодіяти з іншими країнами на спільних засадах.



## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Документ №984\_011 від 27.06.2014 URL: [https://zakon.rada.gov.ua/laws/show/984\\_011#Text](https://zakon.rada.gov.ua/laws/show/984_011#Text)
2. Угода про фінансування заходу "Підтримка ЄС для електронного урядування та цифрової економіки в Україні": Міністерство цифрової трансформації України та Європейський Союз, Документ № 984\_001-20 від 11.02.2020. URL: [https://zakon.rada.gov.ua/laws/show/984\\_001-20#Text](https://zakon.rada.gov.ua/laws/show/984_001-20#Text).
3. Конституція України: офіц. текст. Київ : КМ, 2013. 96 с.– URL: <http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>
4. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/go/435-15>.
5. Податковий кодекс України: Закон України від 02.12.2010 № 2755-VI URL: <https://zakon.rada.gov.ua/laws/show/2755-17#Text>
6. Про електронні довірчі послуги: Закон України від 2017р. №2155-VIII, Відомості Верховної Ради, 2017, № 45, ст.400. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
7. Про електронні документи та електронний документообіг: Закон України від 05.07.1994 р. №2130-IX. Відомості Верховної Ради України № 80/94 ст.275. URL: <http://zakon0.rada.gov.ua/laws/show/851-15>
8. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. №80/94-ВР. Відомості Верховної Ради України №80/94 ст.286. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>



9. Про захист персональних даних: Закон України від 2010р. №2297-VI. Відомості Верховної Ради України № 34. с. 481. URL: <http://zakon5.rada.gov.ua/laws/show/2297-17>
10. Про інформацію: Закон України від 1992 №2657-XII с.650. Відомості Верховної Ради України 1992р. №48 с.650. URL: <http://zakon3.rada.gov.ua/laws/show/2657-12>
11. Деякі питання забезпечення безперебійного функціонування системи надання електронних довірчих послуг: Постанова Кабінету Міністрів України від 17.03.2022 № 300. URL: <https://zakon.rada.gov.ua/laws/show/300-2022-%D0%BF#Text>
12. Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг: Постанова Кабінету Міністрів України від 4 грудня 2019 р. № 1137 URL: <https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#n15>
13. Питання Міністерства цифрової трансформації: Постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856 URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text>
14. Про затвердження Положення про інтегровану систему електронної : Постанова Кабінету Міністрів України від 19 червня 2019 р. № 546. URL: <https://zakon.rada.gov.ua/laws/show/546-2019-%D0%BF#Text>
15. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 8 листопада 2017 р. № 797-р. URL: <https://zakon.rada.gov.ua/laws/show/797-2017-%D1%80#Text>
16. Звіт про фінансові результати за 2019 рік: Міністерство цифрової трансформації України. URL: [Звіт за 2019 рік](#)
17. Звіт про фінансові результати за 2020 рік: Міністерство цифрової трансформації України. URL: [Звіт за 2020 рік](#)
18. Звіт про фінансові результати за 2021 рік: Міністерство цифрової трансформації України. URL: [Звіт за 2021 рік](#)

- 19.Звіт про фінансові результати за 2022 рік: Міністерство цифрової трансформації України. URL: [Звіт за 2022 рік](#)
- 20.Звіт про результати роботи Міністерства цифрової трансформації України в 2022 році: Міністерство цифрової трансформації України №Н54 05.05.2023 URL: [https://cms.thedigital.gov.ua/storage/uploads/files/page/ministry/%D0%97%D0%B2%D1%96%D1%82\\_%D0%9C%D1%96%D0%BD%D1%86%D0%B8%D1%84%D1%80%D0%B8\\_2022.pdf](https://cms.thedigital.gov.ua/storage/uploads/files/page/ministry/%D0%97%D0%B2%D1%96%D1%82_%D0%9C%D1%96%D0%BD%D1%86%D0%B8%D1%84%D1%80%D0%B8_2022.pdf)
- 21.План роботи Міністерства цифрової трансформації України на 2020 рік: Міністерство цифрової трансформації України. URL: <https://thedigital.gov.ua/storage/uploads/files/page/ministry.pdf>
- 22.Бочарова Ю.Г., Чернега О.Б., Кожухова Т.В. Діджиталізація та цифрові трансформації в ЄС: Економіка і організація управління •№ 2 (42) 2021. URL: <https://jeou.donnu.edu.ua/article/view/11026/10925>
- 23.Віховський О. О., Ковтун О. А. Теоретико-концептуальні підходи щодо визначення дефініції "Публічний контроль" в контексті сучасної парадигми публічного управління: Публічне управління і адміністрування в Україні. 2022. № 30. С. 49–53. URL: <http://www.pag-journal.iei.od.ua/archives/2022/30-2022/8.pdf>.
- 24.Ганущин С. Н. Імплементация досвіду Європейського Союзу в українську реальність формування взаємодії між громадянським суспільством та публічним управлінням: Публічне управління і адміністрування в Україні. 2022. № 31. С. 97–101. URL: <http://www.pag-journal.iei.od.ua/archives/2022/31-2022/17.pdf>.
- 25.Голобородько А. Соціально-економічні передумови та чинники розвитку цифрових трансформацій економіки: Вісник, 2022, №4125.
- 26.Демошенко Г. Вплив цифрової трансформації на муніципальне управління: Аспекти публічного управління. 2022. № 1. С. 36–42.
- 27.Доскалов І. С., Ручинська Н. С. Зарубіжний та вітчизняний досвід функціонування системи публічного управління в умовах становлення



- інформаційного суспільства: Інвестиції: практика та досвід. 2021. № 21. С. 111–115. URL: [http://www.investplan.com.ua/pdf/21\\_2021/19.pdf](http://www.investplan.com.ua/pdf/21_2021/19.pdf).
28. Індекс цифрової трансформації регіонів України. Підсумки 2022 року. URL: <https://drive.google.com/drive/folders/1Wp6IaHb0uRKb68mgebq8CvZbgVхupkCz>
29. Карпенко О. В., Карпенко Ю. В. Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансфери: Державне управління: удосконалення та розвиток. 2021. № 10. URL: [http://www.dy.nayka.com.ua/pdf/10\\_2021/4.pdf](http://www.dy.nayka.com.ua/pdf/10_2021/4.pdf).
30. Копанєва, В. О., Костенко, Л. Й., Новицький, О. В., & Резніченко, В. А. Завдання цифрової трансформації науково-інформаційного середовища: Проблеми програмування, 2023.
31. Корчан, В., & Морозова, І. Методи сумісності для ідентифікації пристроїв інтернету речей у гетерогенних мережах зв'язку на базі архітектури цифрових об'єктів: Технічні науки та технології, (2 (32)), 2023р., 235-239.
32. Краус, К. М., Краус, Н. М., & Поченчук, Г. М. Інституціональні аспекти та цифровізація фінансової інклюзії в національній економіці: Innovation and Sustainability, 2022р, № 2: 18–28.
33. Малий І. Й., Цедік М. Г. Інституційний вимір цифровізації державного управління в Україні: Державне управління: удосконалення та розвиток. 2022. № 2. URL: [http://www.dy.nayka.com.ua/pdf/2\\_2022/5.pdf](http://www.dy.nayka.com.ua/pdf/2_2022/5.pdf).
34. Новицький, О. В., Копанєва, В. О., Костенко, Л. Й., & Резніченко, В. А. Завдання цифрової трансформації науково-інформаційного середовища: Problems in programming, 2023р.
35. Опитування НДІ: Можливості та перешкоди на шляху демократичного переходу України: Офіційний сайт Київського міжнародного інституту соціології, 2022. URL: [https://www.kiis.com.ua/materials/pr/20220630\\_m/May%202022%20surv](https://www.kiis.com.ua/materials/pr/20220630_m/May%202022%20surv)



[ey%20-%20NDI%20Ukraine%20-%20Public\\_fin\\_UKR.pdf](#) (дата звернення 10.07.2023)

- 36.Павлишин З. Я. Реформа системи впровадження сучасних технологій інформаційного забезпечення державного управління: Інвестиції: практика та досвід. 2019. № 2. С. 149–154.  
URL: [http://www.investplan.com.ua/pdf/2\\_2019/26.pdf](http://www.investplan.com.ua/pdf/2_2019/26.pdf).
- 37.Павлов М. М. Особливості процесу цифровізації публічного управління в розвинутих країнах: Інвестиції: практика та досвід. 2021. № 15. С. 140–144.  
URL: [http://www.investplan.com.ua/pdf/15\\_2021/23.pdf](http://www.investplan.com.ua/pdf/15_2021/23.pdf).
- 38.Піскоха Н. Цифрова трансформація місцевого самоврядування: визначення поняття та напрямків утворення цифрових громад: Аспекти публічного управління. 2021. № 6. С. 39–45.
- 39.ПриватБанк запустив перші в Україні біометричні pos-термінали: ПриватБанк. URL: <https://privatbank.ua/news/2020/8/10/1270>
- 40.ПриватБанк і Mastercard запускають перший в Україні проєкт поведінкової біометрії: ПриватБанк. URL: <https://privatbank.ua/news/2019/9/16/1018>
- 41.Рогозян Ю.С., Вахлакова В.В. Теоретико-методичні аспекти оцінки результативності й ефективності цифровізації економіки локальних територій України у воєнний і повоєнний час: Академічні візії, Випуск 19/2023. URL: <https://academy-vision.org/index.php/av/article/view/385/346>
- 42.Серьогін С. Публічна служба в умовах цифрової трансформації: завдання, функції та вектори розвитку: Аспекти публічного управління, 2022, № 3, С. 11–20.
- 43.Старикова Г. Демократизація публічного управління: регіональний аспект: Аспекти публічного управління. 2021, № 5, ст. 47–54.
- 44.Цимбал Б. М. Механізм публічного управління безпекою особистості: якісно-новий вимір у системі цифрових технологій та інновацій: Публічне управління і адміністрування в Україні, 2022р., № 30, с. 91–94.  
URL: <http://www.pag-journal.iei.od.ua/archives/2022/30-2022/15.pdf>.

- 45.Цифрова адженда України – 2020: Концептуальні засади (версія 1.0).  
Першочергові сфери, ініціативи, проекти «цифровізації» України до 2020 року: Проект. URL: <https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf>
- 46.Цифрова ідентифікація в Україні та світі: Національний репозитарій академічних текстів, 14 липня 2020р.  
URL:<https://nrat.ukrintei.ua/czyfrova-identyfikacziya-v-ukrayini-ta-sviti/>
- 47.Цифрові трансформації в Україні: чи відповідають вітчизняні інституційні умови зовнішнім викликам та європейському порядку денному?: Поліський фонд міжнародних та регіональних досліджень, 2020р. URL: [http://eap-csf.org.ua/wp-content/uploads/2021/04/Research\\_DT\\_PF\\_WG2\\_ua-1.pdf](http://eap-csf.org.ua/wp-content/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf)
- 48.Цілі до 2024 року: Офіційний сайт Міністерства цифрової трансформації України. URL: <https://thedigital.gov.ua/ministry> (дата звернення 10.07.2023)
- 49.Чалабієва М. Р. Еволюція концепції "Держава у смартфоні" в умовах розвитку сучасного конституціоналізму: Юридичний науковий електронний журнал, 2022, № 5, с. 129–131. URL: [http://lsej.org.ua/5\\_2022/27.pdf](http://lsej.org.ua/5_2022/27.pdf)
- 50.Шевченко С. О., Мунько А. Ю. Управлінські підходи до подолання наслідків пандемії COVID-19 в Україні: Публічне управління і адміністрування в Україні, 2022., № 27. с. 64–67. URL: <http://www.pag-journal.iei.od.ua/archives/2022/27-2022/13.pdf>
- 51.Шевчук І., Депутат Б. Економічний аспект використання хмарних технологій у діяльності органів публічної влади та бізнес-структур: Економіка та суспільство. 2021р. № 31.  
URL: <https://economyandsociety.in.ua/index.php/journal/article/view/689/662>
- 52.Blue, A. (2021). Evaluating Estonian E-residency as a Tool of Soft Power. Place Branding and Public Diplomacy, №17(2020), ст.359–367.  
URL:<https://doi.org/10.1057/s41254-020-00182-3>
- 53.Digital Compass 2030: the European way for the Digital Decade. URL: [https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030\\_en.pdf](https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030_en.pdf)
- 54.«eHealth» (eZdorovya). Офіційний веб-сайт. URL : <https://ehealth.gov.ua>



55. Informationsverige.se. (2023, 22 березня). Банки, банківські послуги та цифрові платіжні сервіси: Управління лену Вестра-Йоталанд. Copyright 2023. URL: <https://www.informationsverige.se/uk/jag-har-fatt-uppehallstillstand/ekonomi-pengar-och-rakningar/bank-och-banktjanster.html>
56. «Helsi. Me». Офіційний веб-сайт. URL : <https://helsi.me/about>.
57. Handy-signatur & bürgerkarte der digitale ausweis: Федеральний канцеляріат Австрії. URL: <https://www.buergerkarte.at/anwendungen-karte.html>
58. Rao Ursula, Nair Vijayanka. "Aadhaar: Governing with Biometrics." Special Section: Aadhaar: Governing India with Biometrics, Pages 469-481, Published online: 22 May 2019. URL: <https://www.tandfonline.com/doi/full/10.1080/00856401.2019.1595343>
59. The Economic Impact of Digital Identity in Canada: Канадська рада з цифрової ідентифікації та автентифікації. URL: <https://diacc.ca/wp-content/uploads/2018/05/Economic-Impact-of-Digital-Identity-DIACC-v2.pdf>

