НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ННІ неперервної освіти

ПОГОДЖЕННЯ **В.о. директора ННІ неперервної освіти**	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ** **В.о. завідувача кафедри публічного управління, менеджменту інноваційної діяльності та дорадництва**
_____ Юлія НЕГОДА	**_____ Ольга ВИТВИЦЬКА**
«____» _____ 2025 р.	«____» _____ 2025 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему «Інноваційні інструменти формування старатегій кібергбезпеки органів державної влади»

Спеціальність 281 «Публічне управління та адміністрування»

Освітня програма «Публічне управління та адміністрування»

Орієнтація освітньої програми освітньо-професійна

Гарант освітньої програми
д.е.н., професор _____ **Олександр ЖЕМОЙДА**
(підпис)

Керівник магістерської кваліфікаційної роботи
д.держ.упр., доцент _____ **Оксана ЄВСЮКОВА**
(підпис)

Виконав _____ **Антон БАЛАНОВ**
(підпис)

КИЇВ – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ННІ неперервної освіти

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
публічного управління, менеджменту
інноваційної діяльності та дорадництва

д.е.н., проф. _____ **Ольга ВИТВИЦЬКА**
"____" _____ 2025 р.

ЗАВДАННЯ ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ СТУДЕНТУ

Баланову Антону Миколайовичу
[прізвище, ім'я, по-батькові]

Спеціальність 281 «Публічне управління та адміністрування»
Освітня програма «Публічне управління та адміністрування»
Орієнтація освітньої програми освітньо-професійна

Тема магістерської кваліфікаційної роботи: **«Інноваційні інструменти формування стратегій кібергбезпеки органів державної влади»**
Затверджена наказом ректора НУБіП України № 9 «С» від 07.01.2025 р.
Термін подання завершеної роботи на кафедру 2025.10.29
Вихідні дані до магістерської кваліфікаційної роботи нормативно-правові акти, монографічна література, наукові статті вітчизняних та зарубіжних вчених
Перелік питань, що підлягають дослідженню:
1. Теоретичні засади формування стратегій кібербезпеки органів державної влади.
2. Аналіз глобальних тенденцій кібербезпеки та організаційно-функціональні засади управління в Україні.
3. Удосконалення стратегії кібербезпеки органів державної влади на основі розвитку системи ідентифікації та інноваційних підходів.

Дата видачі завдання *«10»жовтня 2024 р.*

Керівник магістерської кваліфікаційної роботи **Оксана ЄВСЮКОВА**

Завдання прийняла до виконання _____ **Антон БАЛАНОВ**

ЗМІСТ

РЕФЕРАТ

Магістерська кваліфікаційна робота на тему: «Інноваційні інструменти формування стратегій кібергбезпеки органів державної влади» за структурою складається зі вступу, трьох розділів, висновків та списку використаної літератури. Основна частина складає 103 сторінки комп'ютерного тексту. В роботі міститься 2 таблиці та 28 рисунків. Список використаної літератури складається з 59 найменувань.

Метою дослідження є теоретичне обґрунтування та розробка практичних рекомендацій щодо удосконалення стратегії кібербезпеки органів державної влади України на основі впровадження інноваційних інструментів, зокрема, розвитку системи цифрової ідентифікації та переходу до проактивних моделей захисту.

Об'єктом дослідження є процес формування та реалізації стратегії кібербезпеки в системі публічного управління України.

Предметом дослідження є інноваційні інструменти, методи та концептуальні підходи, що забезпечують удосконалення стратегії кібербезпеки органів державної влади, зокрема розвиток системи цифрової ідентифікації.

Методи дослідження. У процесі підготовки магістерського дослідження було застосовано комплекс взаємодоповнюючих методів: системний підхід дозволив розглянути кібербезпеку органів державної влади як цілісну національну систему; аналіз, синтез та індукція/дедукція використовувалися для формулювання теоретичних положень, систематизації інституційного механізму та виведення загальних стратегічних рекомендацій; функціональний аналіз застосовувався для оцінки ролі суб'єктів управління та обґрунтування ключової функції цифрової ідентифікації; порівняльно-правовий метод був необхідний для зіставлення вітчизняних положень Стратегії кібербезпеки із міжнародними стандартами; а метод моделювання та прогнозування використовувався для теоретичного обґрунтування перспектив

розвитку національної системи на засадах інноваційних підходів (Zero Trust, блокчейн).

Ключові слова**:** ДЕРЖАВНЕ УПРАВЛІННЯ, КІБЕРБЕЗПЕКА, СТРАТЕГІЯ КІБЕРБЕЗПЕКИ, ОРГАНИ ДЕРЖАВНОЇ ВЛАДИ, ЦИФРОВА ІДЕНТИФІКАЦІЯ, БЛОКЧЕЙН, БІОМЕТРІЯ, КІБЕРСТІЙКІСТЬ, МУЛЬТИФАКТОРНА АВТОЕНТИФІКАЦІЯ.

ВСТУП

Актуальність теми дослідження. У сучасному світі інформаційна безпека держави стає одним із ключових чинників її стійкості та розвитку. Кіберзагрози, такі як кібератаки, кібершпигунство, кібертероризм, кіберсаботаж, дезінформація, постійно зростають, що робить необхідним розробку та впровадження ефективної стратегії кібербезпеки. Україна, як і інші країни світу, стикається з численними кіберінцидентами, які можуть мати значний вплив на її політику, економіку та суспільство.

Інформаційна безпека є одним із ключових факторів стійкості та розвитку держави. Кібербезпека є невід'ємною складовою інформаційної безпеки. У сучасному світі кіберзлочинність та кібератаки постійно зростають за масштабами та складністю. Україна перебуває у складному геополітичному середовищі, що може сприяти кібератакам та іншим формам цифрової агресії з боку інших країн.

Війна в України, яка розпочалась у 2014 році, стала складним гібридним конфліктом, включаючи збройні дії, інформаційну війну та кіберагресію. Військові дії супроводжуються активними кібератаками та інформаційною війною.

В умовах збройної агресії та в контексті стратегії кібербезпеки Україна приділяла значну увагу захисту своїх критичних інформаційних інфраструктур та протидії кіберзагрозам. Попередньо, ключові аспекти стратегії включали захист критичних інфраструктур, розвиток кіберзахисту, інформаційну безпеку, міжнародне співробітництво, експертну та освітню роботу. Зусилля зосереджувались на захисті критичних об'єктів, таких як енергетичні системи, телекомунікаційні мережі, фінансові установи тощо від кібератак. Створювались та вдосконалювались систем кіберзахисту, які включають в себе розробку захисного програмного забезпечення, моніторинг та реагування на кіберінциденти. Проводилась робота із запобіганню

дезінформації та пропаганді, яка може посилити дестабілізацію суспільства та підірвати довіру до державних інституцій. Відбувалось посилення взаємодії з міжнародними партнерами та організаціями з метою обміну інформацією та кращого реагування на кіберзагрози. Проводились заходи із підвищення рівня кіберграмотності населення та професіоналів у сфері кібербезпеки, щоб покращити виявлення та реагування на кіберзагрози.

Україна активно формується цифрова економіка, що робить її ще більш уразливою перед кіберзагрозами. Збільшення кількості підключених до Інтернету пристроїв і послуг також збільшує потенційні точки вразливості. Нові технології, такі як штучний інтелект, Інтернет речей (IoT), блокчейн тощо, принесли не лише нові можливості, але й нові загрози для кібербезпеки. Втрата довіри до інформаційних систем та ресурсів може призвести до значних економічних та соціальних проблем.

Інформаційні операції та пропаганда в інтернеті стали невід'ємною частиною сучасної гібридної війни. Досвід показує, що з початком повномасштабного вторгнення, правильна стратегія кібербезпеки може визначати інформаційну перевагу. Чинна Стратегія кібербезпеки України затверджена у 2016 році [1]. За цей час ситуація у сфері кібербезпеки значно змінилася, тому виникла потреба у вдосконаленні Стратегії. Впровадження ефективної Стратегії кібербезпеки стає критично важливим завданням для України, яке має на меті захистити національні інтереси та забезпечити стійкість інформаційної і кібернетичної інфраструктури держави.

Проблематика, що охоплює найрізноманітні аспекти формування стратегії кібербезпеки та забезпеченні інформаційної безпеки досліджувалися у наукових працях вітчизняних вчених, а саме: І. В. Арістова., І. Р Березовської., О. П. Дзьобаня, Р.А. Калюжного, Б. А. Кормича, В. А.Ліпкана, А. І. Марущак, В. С. Цимбалюка, О. К. Юдіна , а також регламентуються численними законами, указами та доктринами [1-14].

Разом з тим, продовжує залишатись актуальною необхідність у подальших дослідженнях низки питань щодо ефективності реалізації Стратегії. Проблеми, перераховані вище, їх актуальність обумовили вибір теми магістерського дослідження, визначили її мету й завдання.

Мета і завдання дослідження. є теоретичне обґрунтування та розробка практичних рекомендацій щодо удосконалення стратегії кібербезпеки органів державної влади України на основі впровадження інноваційних інструментів, зокрема, розвитку системи цифрової ідентифікації та переходу до проактивних моделей захисту.

Для досягнення поставленої мети у процесі дослідження було поставлено та вирішено наступні *завдання:*

- уточнити сутність, принципи і стратегічну функцію кібербезпеки в системі державного управління;
- проаналізувати функції ключових суб'єктів (НЦУ, ДССЗЗІ, СБУ та ін.) у сфері протидії кіберзлочинам;
- обґрунтувати роль цифрової ідентифікації, як ключового фактора забезпечення кібербезпеки та основи для встановлення довіри в публічному управлінні;
- провести аналіз сучасного стану кібербезпеки та тенденцій кіберзлочинності;
- оцінити поточний вплив Стратегії кібербезпеки України на забезпечення інформаційної безпеки держави та виявити основні прогалини;
- сформулювати пріоритети забезпечення конфіденційності та безпеки даних цифрової ідентифікації в публічному управлінні.

Об’єктом дослідження є цифровізація органів державної влади, як процес.

Предметом дослідження є інноваційні інструменти, методи та концептуальні підходи, що забезпечують удосконалення стратегії кібербезпеки органів державної влади.

Методи дослідження. Для досягнення мети та виконання завдань дослідження був застосований комплекс взаємодоповнюючих методів: системний підхід дозволив розглянути кібербезпеку органів державної влади як цілісну національну систему; аналіз, синтез та індукція/дедукція використовувалися для формулювання теоретичних положень, систематизації інституційного механізму та виведення загальних стратегічних рекомендацій; функціональний аналіз застосовувався для оцінки ролі суб'єктів управління (Мінцифра) та обґрунтування ключової функції цифрової ідентифікації; порівняльно-правовий метод був необхідний для зіставлення вітчизняних положень Стратегії кібербезпеки із міжнародними стандартами; а метод моделювання та прогнозування використовувався для теоретичного обґрунтування перспектив розвитку національної системи на засадах інноваційних підходів (Zero Trust, блокчейн).

Структура та обсяг роботи. Магістерська кваліфікаційна робота складається із вступу, трьох розділів, висновків та списку використаних джерел. Повний обсяг роботи складає 110 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ФОРМУВАННЯ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

1.1. Поняття, сутність та принципи кібербезпеки в державному секторі

Кібербезпека за умов сьогодення є стратегічною проблемою міжнародного значення, яка зачіпає всі верстви населення держав світу. Державна політика з інформаційної та кібербезпеки перетворюється на засіб посилення національної безпеки і надійності інформаційних систем держави. Стратегії кібербезпеки були прийняті такими державами як: США, Швеція, Естонія, Фінляндія, Чехія, Франція, Німеччина, Литва, Великобританія, Канада, Японія, Індія, Австралія, Нова Зеландія, Колумбія тощо. Цей список країн наочно показує, що проблема кібербезпеки визнається актуальною в усьому світі.

Не залишилась осторонь цієї проблеми й Україна, яка схвалила Стратегію кібербезпеки. Цей документ окреслює пріоритети та напрями кібербезпеки, які є основою для розробки політики інформаційної безпеки, що відповідає міжнародним стандартам. Одним із важливих завдань на сучасному етапі є захист об’єктів критичної інфраструктури, що є предметом турботи багатьох країн світу. Захист критичної інфраструктури передбачає заходи, спрямовані на забезпечення безпеки тих взаємозалежних систем, мереж та активів, які є основою для функціонування життєво важливих служб і сфер суспільного життя. Об’єкти критичної інфраструктури можуть бути як військовими, так і цивільними, а також мають можливість подвійного призначення, що особливо важливо в умовах сучасних загроз. До життєво важливих об’єктів матеріальної інфраструктури можна віднести різноманітні елементи, такі як дороги, мости, аеропорти, споруди зв’язку, електростанції, а також банківська система, медичні послуги, виробництво і розподіл

електроенергії, державні аварійно-рятувальні служби, повітряні та наземні перевезення. Захист цих об’єктів є критично важливим для забезпечення стабільного функціонування держави та забезпечення національної безпеки.

З аналогічного приводу у Резолюції Ради Безпеки ООН S/RES/2341 (2017) «Про захист критичної інфраструктури» від 13 лютого 2017 р. зазначається, що «кожна держава сама визначає, які об’єкти її інфраструктури є критично важливими і як забезпечити їх ефективний захист…» [25].

Таким чином, підходи до визначення сегментів критичної інфраструктури можуть варіюватися залежно від країни. Наприклад, у США до цієї категорії, окрім традиційних об’єктів, що забезпечують життєдіяльність суспільства, відносяться й такі як національні пам’ятники, виборча система, дипломатичні місії, що робить їх уразливими для потенційних кібератак. В умовах сучасного інформаційного суспільства критична інфраструктура не може функціонувати без інформаційної інфраструктури, яка включає комп’ютерні системи та мережі, зокрема системи диспетчерського управління і збору даних. Взаємозалежність цих систем дозволяє ефективно обмінюватися інформацією та здійснювати необхідний аналіз для забезпечення стабільного функціонування критично важливих функцій.

Застосування технологій дистанційного управління сприяє підвищенню ефективності та зменшенню витрат, але одночасно відкриває критичну інфраструктуру для кіберзагроз. Сучасна геополітична ситуація, в якій кібератаки на критичну інфраструктуру можуть мати значні військові наслідки, перетворює кібербезпеку на важливий аспект національної оборони. Вимкнення електростанцій, знищення нафтопроводів або припиненняпостачання води можуть призвести до серйозних економічних та соціальних наслідків, а отже, надати значну перевагу агресору. Такі кібератаки

є не лише загрозою для стабільності країни, але й можуть підірвати її національну безпеку.

Україна, як і багато інших країн, стала жертвою інформаційної агресії, зокрема з боку російської федерації. В умовах війни росія активно використовує інформаційно-психологічні операції для пропаганди сепаратизму, насильства та міжнаціональної ворожнечі, з метою підриву національної ідентичності та територіальної цілісності України. Це негативно впливає не лише на внутрішню політику країни, але й на міжнародний імідж України. Інформаційно-психологічні кампанії спрямовані на зміну суспільної свідомості не тільки громадян України, а й на світову громадськість, зокрема через пропаганду в медіа.

Окрім того, Україна одночасно з іншими державами 27 червня 2017 р. зазнала найбільшої хакерської атаки, яка поширила вірус Petya A. Цей інцидент став важливим сигналом для України і інших країн світу про масштаби і серйозність кіберзагроз. Хакерська атака з використанням вірусу Petya.A показала, наскільки уразливою може бути національна інфраструктура в умовах сучасних кібервикликів. Вірус не лише порушив роботу державних установ, таких як КМУ та Національна поліція, але й завдав значної шкоди важливим об’єктам критичної інфраструктури, включаючи аеропорт «Бориспіль», Чорнобильську атомну електростанцію, а також фінансові установи та енергетичні компанії. Подібні кібератаки відбувають особливо інтенсивно, починаючи з 2022 року.

Кібератака підтвердила необхідність посилення кіберзахисту та розвиток механізмів швидкого реагування на подібні загрози. Важливим аспектом є інтеграція сучасних технологій, таких як системи моніторингу кіберзагроз і швидкого реагування, а також міждержавне співробітництво для протидії міжнародним кіберзлочинам. Також, кібератака призводить до

зараження комп’ютерів по всьому світу (США, Великобританія, Німеччина, Польща, Литва та ін.) і завдає збитків приблизно на 8 млрд доларів США.

Наслідки таких кібератак підкреслюють важливість формування національних та міжнародних стандартів безпеки для захисту критичних інформаційних та інфраструктурних об’єктів від кіберзагроз.

Виходячи із наведеного, варто визначити структурні елементи стратегічного управління інформаційної безпеки України на міжнародному та загально-державному рівнях. На нашу думку, вони повинні включати: а)захист відомостей, що містять державну або комерційну таємницю; б) технічний захист серверів державних установ та систем життєзабезпечення; в) захист безпеки даних, як набір апаратних та програмних засобів, що забезпечують збереження інформації від неавторизованого доступу; г) інформаційно-психологічний блок, який передбачає реалізацію систем заходів, спрямованих на захист від цілеспрямованого впливу на населення, його психологічний стан або імідж на міжнародній арені; д) наукову складову, покликану знаходити нові та вдосконалювати існуючі методи та засоби забезпечення інформаційної та кібербезпеки; є) освітні програми серед населення для збільшення медіа-досвідченості та медіа-стійкості.

Аналіз спеціалізованої літератури з приводу трактування поняття кібербезпека» дозволило виокремити ключові підходи до трактування змісту цієї дефініції (табл. 1.1).

Вона охоплює як технічні, так і організаційні аспекти, зокрема створення надійних механізмів ідентифікації, управління ризиками, моніторингу та реагування на інциденти у цифровому середовищі.

У сучасних умовах кібербезпека є ключовим компонентом національної безпеки, оскільки забезпечує стійкість до загроз, таких як несанкціонований доступ, кібершпигунство, шкідливе програмне забезпечення, а також атаки на критичну інфраструктуру.

Таблиця 1.1.

Трактування змісту дефініції «кібербезпека» у вітчизняній науковій літературі

Автори, рік, джерело	Характеристика поняття
1	2
Закон України «Про основі засадизабезпечення кібербезпеки України» [18]	«…кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».
Павленко В. [23, с.31]	«…кібербезпека – діяльність, спрямованої на захист систем, мереж і комп'ютерних програм від цифрових атак».
Баранов О. [6, с.31]	«…кібербезпека – інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж. кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації».
Мельник С. Тихомиров О., Лєнков О. [23]	«…кібербезпека може визначатися як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам».
Фурашев В. [46]	«…кібербезпека – це стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого несвідомого, негативного впливу (управління) інформації».
Шеломевцев В. [52]	«…кібербезпека – сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються».
Діордіца І. [29]	«…кібербезпека – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі з метою забезпечення кібернетичної безпеки інформаційних, телекомуніка ційних та інформаційно-телекомунікаційних систем».
Логінова Н. [50, с.575]	«…кібербезпека – стан захищеності державних електронних інформаційних ресурсів у кібер-просторі від ризику стороннього впливу, виявлення та запобігання різних зовнішніх втручань».
Ліпкан В. [49]	«…кібербезпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кібернетичному просторі, в якому є можливим безперешкодне створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, а у вузькому сенсі -стан індивіда, суспільства та держави, де відсутня будь-яка небезпека».
Горлинський В., Горлинський Б. [19]	«…кібербезпека підсистемного утворення інформаційної безпеки».
Сироватченко М. [35]	«…кібербезпека – це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або пере- даються, і пов'язаних з ними послуг, які ці системи пропонують або роблять доступними».

Джерело: побудовано автором на основі наукових джерел.

Особливістю кібербезпеки є її динамічний і комплексний характер, що зумовлює необхідність адаптації до швидко змінюваних технологій і нових форм кіберзлочинності.

Водночас кібербезпека вимагає міжгалузевого підходу, інтеграції знань і досвіду з різних сфер, таких як інформаційні технології, право, економіка та соціологія. У контексті державної політики, кібербезпека передбачає не лише захист наявних систем, але й активну розробку та впровадження превентивних заходів, підвищення кіберсвідомості громадян, розвиток міжнародного співробітництва та постійне вдосконалення нормативно- правової бази, що дозволяє створювати ефективну та стійку систему протидії сучасним викликам у кіберпросторі (табл. 1.2.).

Таблиця 1.2.

Узагальнення змісту та компонентів поняття «Кібербезпека»

Визначення	Цілі та задачі	Компоненти
Стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кібернетичному просторі/ у сфері функціонування інформаційно-телекомунікаційних систем	Діяльність, спрямована на захист систем, мереж і комп'ютерних програм від цифрових атак	Сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів
Інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж	Здатність людини, суспільства і держави щодо запобігання негативного впливу (управління) інформації	Підсистемне утворення інформаційної безпеки

Джерело: побудовано автором на основі аналізу наукових джерел.

Отже, аналіз змістовної сутності дефініції «кібербезпека» у вітчизняних наукових джерелах показує, що поняття розглядається як багатокомпонентне та динамічне. Більшість авторів визначають кібербезпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави у кіберпросторі, пов'язаний із запобіганням та нейтралізацією цифрових загроз. Частина дослідників трактує її як діяльність або сукупність технічних та

організаційних заходів, спрямованих на захист інформаційних систем, мереж і даних від атак та несанкціонованого доступу. Окремі автори включають до змісту поняття інформаційно-психологічний та управлінський виміри, розглядаючи кібербезпеку як здатність протидіяти негативному впливу й забезпечувати цілісність інформаційних процесів. У наукових підходах також простежується розуміння кібербезпеки як елемента або підсистеми ширшої інформаційної безпеки.

Узагальнення дозволяє визначити, що кібербезпека охоплює три ключові аспекти: 1) стан захищеності, 2) процес/діяльність із забезпечення захисту, 3) система суб'єктів, методів і засобів.

Таким чином, у сучасній українській науковій літературі кібербезпека постає як комплексна категорія, що поєднує технічні, правові й організаційні механізми та є важливою складовою національної безпеки України.

1.2. Інституційний механізм державного управління у сфері кібербезпеки та протидії кіберзлочинності

Розбудову інституційного механізму державного управління в сфері протидії кіберзлочинам пропонується розпочати з ідентифікації суб'єктів такого управління або державних інституцій. Аналіз повноважень чинних вищих та центральних органів влади в Україні дозволив визначити такий їх склад: Президент України (ПУ); Верховна Рада України (ВРУ); Рада національної безпеки та оборони України (РНБОУ); Державна служба спеціального зв'язку та захисту інформації (ДССЗЗІ); Кабінет Міністрів України (КМУ); Національна поліція України (НПУ); Служба безпеки України (СБУ); Державне бюро розслідувань (ДБР); Міністерство внутрішніх справ України (МВСУ); (МІПУ). Міністерство культури та стратегічних комунікацій України. (МКСК).

Президент України, відповідно до Конституції України та ЗУ «Про національну безпеку України» [41]: гарантує національну безпеку країни загалом та її складових, зокрема і кібербезпеку; керує РНБО України, що опікується питаннями національної безпеки загалом та кібербезпеки зокрема; схвалює своїм підписом або накладає вето щодо законодавчих актів, прийнятих ВРУ (у тому числі ті, щодо кібербезпеки та протидії кіберзлочиніам).

Верховна Рада України згідно вітчизняного законодавства має такі повноваження в межах державного управління в сфері протидії кіберзлочинам [41]: приймає закони України, у тому числі стосовно кібербезпеки та протидії кіберзлочинам; контролює діяльність КМУ, утому числі в сфері кібербезпеки та протидії кібезлочинності.

РНБО України має такі повноваження в сфері управління кібербезпекою та протидією кіберзлочинністю [41]: «розробляє та розглядає на своїх засіданнях питання, належать до сфери національної безпеки в цілому та кібербезпеки зокрема і надає пропозиції Президентові України, приймає рішення щодо: визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення кібербезпеки; проектів державних програм, доктрин, законів України, указів Президента України, директив Верховного Головнокомандувача Збройних Сил України, міжнародних договорів, інших нормативних актів та документів з питань кібербезпеки; удосконалення системи забезпечення кібербезпеки, утворення, реорганізації та ліквідації органів виконавчої влади у цій сфері; проекту ЗУ «Про Державний бюджет України» та пропозицій до Бюджетної декларації по статтях, пов'язаних із забезпеченням кібербезпеки; матеріального, фінансового, кадрового, організаційного та іншого забезпечення виконання заходів з питань кібербезпеки; заходів різного характеру згідно масштабу потенційних та реальних загроз кібербезпеці України; доручень, пов'язаних з

вивченням конкретних питань та здійсненням відповідних досліджень у сфері кібербезпеки, органам виконавчої влади та науковим закладам України; залучення контрольних, інспекційних та наглядових органів, що функціонують у системі виконавчої влади, до здійснення контролю за своєчасністю та якістю виконання прийнятих РНБО України рішень, введених в дію указами Президента України; забезпечення і контролю надходження та опрацювання необхідної інформації, її збереження, конфіденційності та використання в інтересах кібербезпеки України, аналізу на її основі стану і тенденції розвитку подій, що відбуваються в Україні і в світі, визначення потенційних та реальних загроз кібербезпеці України; невідкладних заходів із розв'язання кризових ситуацій, що загрожують нкібербезпеці України; координує виконання прийнятих РНБО України рішень, введених в дію указами Президента України, і здійснює поточний контроль діяльності органів виконавчої влади у сфері кібербезпеки, подає Президентові України відповідні висновки та пропозиції; ініціює розроблення нормативних актів та документів з питань кібербезпеки, узагальнює практику їх застосування та результати перевірок їх виконання; координує і контролює діяльність органів виконавчої влади з протидії кіберзлочинам в межах забезаеченя кібербезпеки країни».

КМУ в свою чергу в межах державного управління протидією кібелочинності [41]: «забезпечує здійснення політики держави, виконання Конституції і законів України, актів Президента України в сфері кібербезпеки та протидії кіберзлочинності; здійснює заходи щодо забезпечення кібербезпеки України, боротьби зі кіберзлочинністю; спрямовує і координує роботу міністерств, інших органів виконавчої влади, що задіяні в процесі управління протидією кіберзлочинам».

Державна служба спеціального зв'язку та захисту інформації згідно вітчизняного законодавства здійснює [16]: «формування та реалізація державної політики у сферах кіберзахисту, активної протидії агресії у

кіберпросторі; реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснення державного контролю в цих сферах; формування загальних вимог до кіберзахисту об'єктів критичної інфраструктури; створення та забезпечення функціонування системи активної протидії агресії у кіберпросторі; створення та забезпечення функціонування Центру активної протидії агресії у кіберпросторі; виконання інших завдань, передбачених законодавством у сфері забезпечення кібербезпеки та кіберзахисту».

Національна поліція України в межах державного управління протидією кіберзлочинам виконує такі завдання [7]: «проводить різни види діяльності на запобігання вчиненню кіберзлочинів; виявляє причини та умови вчинення кіберзлочинів, вживає заходи на виявлення таких злочинів та припиняє їх; здійснює досудове розслідування кіберзлочинів; розшукує кіберзлочинців, що переховуються від оргівн досулвого розслідування, слітдчого судді, суду, ухиляються від виконання кримінального покарання; доствляє зариманих кібезлочинців у місця обмеження свободи та їх тимчасового утримання; здійснює протидію злочинним посяганням на об'єкти критичної інфраструктури, які загрожують їх кібербезпеці, а також захист об'єктів критичної інфраструктури, інтересів суспільства і держави від злочинних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів проти об'єктів критичної інфраструктури; здійснює у визначеному законом порядку протидію злочинним посяганням на об'єкти критичної інфраструктури, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення; захист об'єктів критичної інфраструктури, інтересів суспільства і держави від злочинних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів проти об'єктів критичної інфраструктури; утримує в ізоляторах тимчасового тримання осіб, затриманих

за вчинення кіберзлочинах, осіб, стосовно яких як запобіжний захід застосовано тримання під вартою, осіб, підданих адміністративному арешту, а також обвинувачених і засуджених; здійснює конвоювання осіб, затриманих за підозрою в учиненні кібер правопорушення, узятих під варту, обвинувачених або засуджених до позбавлення волі, а також охороняє їх у залі суду».

СБУ згідно законодавства виконує такі повноваження [3]: «здійснює інформаційно-аналітичну роботу в інтересах ефективного проведення органами державної влади та управління України внутрішньої і зовнішньої діяльності, пов'язаної з кібербезпекою України; здійснює заходи контррозвідувального забезпечення кібербезпеки суб’єктів нашої держави за кордоном; виявляє, припиняє та розкриває кримінальні кіберправопорушення, розслідування яких віднесено законодавством до компетенції СБУ, проводити їх досудове розслідування; розшукувати осіб, які переховуються у зв'язку із вчиненням зазначених кримінальних кіберправопорушень; здійснює профілактику правопорушень у сфері кібербезпеки; надає допомогу органам Національної поліції України, іншим правоохоронним органам у боротьбі із вчиненням кримінальних кіберправопорушень; виконує за дорученням Президента України інші завдання, безпосередньо спрямовані на забезпечення внутрішньої та зовнішньої кібербезпеки держави».

Державне бюро розслідувань, згідно вітчизняного законодавства, виконує в межах державного управління протидією кібербезпекою такі повноваження [69]: «бере участь у формуванні та реалізації державної політики у сфері протидії кіберзлочинності, вносить відповідні пропозиції на розгляд КМУ; здійснює інформаційно-аналітичні заходи щодо встановлення системних причин та умов проявів організованої кіберзлочинності вживає заходів до їх усунення; припиняє і розкриває відповідні кримінальні кіберправопорушення; здійснює оперативно-розшукову діяльність та

досудове розслідування відповідних кримінальних кіберправопорушень; розробляє і затверджує методику розслідування окремих видів кримінальних кіберправопорушень; вживає заходів щодо відшкодування завданих державі збитків і шкоди, забезпечує можливості для конфіскації коштів та іншого майна, одержаного внаслідок вчинення кримінальних кіберправопорушень; вживає заходів для повернення в Україну з-за кордону коштів та іншого майна, одержаних внаслідок вчинення відповідних кримінальних кіберправопорушень».

МВС України, в свою чергу, відповідно до законодавства наділено такими повноваженнями в сфері протидії кіберзрлочиності [7]: «забезпечує формування державної політики у сфері протидії кіберзлочинності, а також надання поліцейських послуг».

І нарешті Міністерство культури та стратегічних комунікацій України України забезпечує формування та реалізація державної політики у сфері інформаційної безпеки [24, 65]: «є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах культури, державної мовної політики, популяризації України у світі, державного іномовлення, інформаційного суверенітету України (у частині повноважень з управління цілісними майновими комплексами державного підприємства «Мультимедійна платформа іномовлення України» та Українського національного інформаційного агентства «Укрінформ») та інформаційної безпеки, а також забезпечує формування та реалізацію державної політики у сферах відновлення та збереження національної пам’яті, мистецтв, охорони культурної спадщини, музейної справи, вивезення, ввезення і повернення культурних цінностей».

Зростаючий обсяг кіберзлочинності загалом та в умовах воєнного сану, що пов’язано також з агресією проти України і зловмисних дій ворога, детермінує необхідність утворення окремого центрального органу виконавчої

влади правоохоронного характеру, на який мають бути покладені завдання із протидії кіберзлочинності та охороні кібербезпеки – Державного бюро кібербезпеки. Зважаючи на вищевказане та попередньо сформований склад функцій державного управління протидією кіберзлочинам: Президент України здійснює організаційну, інституційну, безпекову, захисну функції; ВРУ – організаційну, інституційну, безпекову, захисну, контрольну функції; РНБО, Державна служба спеціального зв'язку та захисту інформації – прогностично-планову, організаційну, інституційну, безпекову, захисну, контрольну функції; КМУ – прогностично-планову, керівну, організаційну, інституційну, безпекову, інформаційну, економічну; Державне бюро кібербезпеки, Національна поліція України, СБУ, Державне бюро розслідувань – прогностично-планову, керівну, організаційну, контрольну, інституційну, діяльнісну, захисну, безпекову, інформаційну, економічну, правову функції; Міністерство внутрішніх справ України та Міністерство культури та стратегічних комунікацій України – прогностично-планову, організаційну, контрольну функції.

Інституційний механізм державного управління протидією кібезлочинам набуває такого вигляду (Додаток А). Реалізація на практиці вказаного механізму дозволить підвищити ефективність боротьби з кіберзлочинністю та підвищити рівень кібербезпеки країни. Його розширення полягає в необхідності утворення ДБР, яке на відміну від Кіберполіції Національної поліції України буде мати ширші функції, які стосуються кіберзлочинів, що є особливо важкими та впливають на національну безпеку держави. До завдань Державного бюро кібербезпеки пропонується віднести: виявлення ризиків та загроз кібербезпеки країни, їх оцінка та мінімізація і усунення; розробка заходів з гармонізації національної системи протидії кіберзлочинності директивам ЄС; формування проектних пропозицій до нормативно- правових актів з питань попередження кібезлочинності в системі

загроз національній безпеці держави; досягнення кібербезпеки країни шляхом запобігання, виявлення, припинення, розслідування кіберзлочинів; узагальнення та аналіз інформації щодо кіберзлочинів та визначення засобів упередження їх на майбутнє; планування заходів у сфері протидії кіберзлочинів; формування аналітичних висновків і рекомендацій для державних органів усіх рівнів задля підвищення ефективності прийняття ними управлінських рішень в сфері кібербезпеки.

Для забезпечення високої ефективності діяльності Державного бюро кібербезпеки є визначення його повноважень, зокрема: пряма взаємодія із суб'єктами забезпечення кібербезпеки ЄС; як в частинні розслідування кіберзлочинів так в частинні гармонізації державної політики; пряма взаємодія із міжнародними поліцейськими організаціями, зокрема Інтерпол та Європол в частинні розсування кіберзлочинів та інших видів злочинів, що пов'язанні із застосування інформаційних технологій; взаємодія із Державною службою спеціального зв'язку та захисту інформації в частинні технічної підтримки забезпечення кібербезпеки держави та розслідування кіберзлочинів; проведення або участь в здійсненні спеціальних перевірок осіб, які претендують на зайняття керівних посад в системі державного управління або інших посад з високим рівнем корупційного ризику; пряма взаємодія із НАБУ в частинні розслідування корупційних злочинів пов'язаних із криптовалютою; взаємодія із правоохоронними країн ЄС щодо розслідування кіберзлочинів як транснаціональних злочинів; участь в тимчасових слідчих групах з розслідування злочинів, що є загрозами національній безпеці; формування аналітичних довідок для Президента України, Прем'єр Міністра України, Голови Верховної Ради України, про стан кіберзагроз та їх вплив на національну безпеку України.

Отже, проведене дослідження сприяло розвитку інституційних положень державного управління в сфері протидії кіберзлочинам через

формування інституційного механізму останнього, в якому: Президент України здійснює організаційну, інституційну, безпекову, захисну функції; ВРУ – організаційну, інституційну, безпекову, захисну, контрольну функції; РРНБО, Державна служба спеціального зв'язку та захисту інформації – прогностично-планову, організаційну, інституційну, безпекову, захисну, контрольну функції; КМУ – прогностично-планову, керівну, організаційну, інституційну, безпекову, інформаційну, економічну; Державне бюро кібербезпеки, Національна поліція України, СБУ, ДБР – прогностично-планову, керівну, організаційну, контрольну, інституційну, діяльнісну, захисну, безпекову, інформаційну, економічну, правову функції; МВС України та МКСК України – прогностично-планову, організаційну, контрольну функції

1.3. Цифрова ідентифікація як ключовий фактор забезпечення кібербезпеки в системі публічного управління

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]

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. 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 і 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 проектів:

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 Сингапурі 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 проект 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]

Вказані 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, як демократичної країни, 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 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 проектах 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. Варто вказати, 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: ЗУ «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 «держава 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], ЗУ «Про інформацію» [10], ЗУ «Про захист інформації в інформаційно-комунікаційних системах» [8], ЗУ «Про електронні документи та електронний документообіг» [7], ЗУ «Про захист персональних даних» [9], цим Законом, а також іншими нормативно-правовими актами.

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 ВР схвалила ЗУ «Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та ЄС про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства ЄС у сфері електронної ідентифікації» [20].

Отже, проведене дослідження сприяло розвитку інституційних положень державного управління в сфері протидії кіберзлочинам через формування інституційного механізму останнього, в якому: Президент України здійснює організаційну, інституційну, безпекову, захисну функції; ВРУ – організаційну, інституційну, безпекову, захисну, контрольну функції; Рада національної безпеки та оборони України, Державна служба спеціального зв'язку та захисту інформації – прогностично-планову, організаційну,

інституційну, безпекову, захисну, контрольну функції; Кабінет Міністрів України – прогностично-планову, керівну, організаційну, інституційну, безпекову, інформаційну, економічну; Державне бюро кібербезпеки, Національна поліція України, Служба безпеки України, Державне бюро розслідувань – прогностично-планову, керівну, організаційну, контрольну, інституційну, діяльнісну, захисну, безпекову, інформаційну, економічну, правову функції; Міністерство внутрішніх справ України та МКСК України – прогностично-планову, організаційну, контрольну функції.

Висновки до 1 розділу:

1. Варто зазначити, що аналіз змісту поняття «кібербезпека» у вітчизняних наукових джерелах засвідчує, що воно розглядається за структурною ознакою, як багатокомпонентне та динамічне. Значна кількість науковців визначають кібербезпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави у кіберпросторі, пов’язаний із запобіганням та нейтралізацією цифрових загроз. Частина дослідників трактує її як діяльність або сукупність технічних та організаційних заходів, спрямованих на захист інформаційних систем, мереж і даних від атак та несанкціонованого доступу. Відповідно, узагальнюючи вказані підходи та наукові точки зори, на нашу думку, зміст поняття «кібербезпека» охоплює три ключові аспекти, як: стан захищеності, процес/діяльність із забезпечення захисту, систему суб’єктів, методів і засобів. Відтак, варто зробити висновок, що у сучасній українській науковій літературі кібербезпека постає як комплексна категорія, що поєднує технічні, правові й організаційні механізми та є важливою складовою національної безпеки України.

2. Досліджуючи предмет кваліфікаційної (магістерської) роботи, нами доведено, що на основі інституційних положеннь державного управління в сфері протидії кіберзлочинам, варто сформувати інституційний механізм, у

складі якого: Президент України здійснює організаційну, інституційну, безпекову, захисну функції; ВРУ – організаційну, інституційну, безпекову, захисну, контрольну функції; РНБО, Державна служба спеціального зв’язку та захисту інформації – прогностично-планову, організаційну, інституційну, безпекову, захисну, контрольну функції; КМУ – прогностично-планову, керівну, організаційну, інституційну, безпекову, інформаційну, економічну; Державне бюро кібербезпеки, Національна поліція України, СБУ, ДБР – прогностично-планову, керівну, організаційну, контрольну, інституційну, діяльнісну, захисну, безпекову, інформаційну, економічну, правову функції; МЗС України та Міністерство культури та стратегічних комунікацій України – прогностично-планову, організаційну, контрольну функції

3. Визначено, що 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. Цифрова ідентифікація не обмежується лише технічними аспектами. Вона також пов'язана з публічним контролем, прозорістю та громадською участю у владних процесах.

4. На основі аналізу кращих зарубіжних практик таких країн, як: Естонія, Швеція, Сингапур, Канада, Бельгія, австрія загальнено, що серед основних факторів, які впливають на процес цифровізації державного управління та цифрової трансформації суспільства в зарубіжних країнах, варто виділити такі чинники, як: особливості ринкової економіки, які проявляють себе у збільшенні свободи підприємництва, вільний рух робочої сили та конкурентності на ринку праці; розвиток громадянського суспільства та соціального партнерства в цифровому середовищі; децентралізацію влади та впровадження ефективних структурних і регіональних політик.

РОЗДІЛ 2. АНАЛІЗ ГЛОБАЛЬНИХ ТЕНДЕНЦІЙ КІБЕРБЕЗПЕКИ ТА ОРГАНІЗАЦІЙНО-ФУНКЦІОНАЛЬНІ ЗАСАДИ УПРАВЛІННЯ В УКРАЇНІ

2.1. Глобальний аналіз стану кібербезпеки та кіберзлочинності

За останні десятиліття глобальна кіберзлочинність стала однією з найбільших загроз сучасної економіки, створюючи значні виклики для державних і приватних інституцій. Ці загрози проявляються в різних формах, включаючи окремі випадки або скоординовані дії, атаки на основі програмного забезпечення, фізичне втручання, а також зовнішні або внутрішні порушення, спрямовані на національні цифрові мережеві системи. Експерти *Cybersecurity Ventures* оцінюють втрати від кіберзлочнності у 2024 р. у понад 9,5 трлн дол. США. Якщо даний розмір збитків виміряти як країну, то кіберзлочинність може бути третьою за величиною економікою світу після Китаю та США. За прогнозами даної світової організації збитки від кіберзлочинності збільшаться на 15% протягом двох наступних років та дорівнюватимуть 10,5 трлн дол. США у 2025 р. Варто зазначити, що у 2016 р. сума збитків від кібератак становила 3 трлн дол. США

Згідно даних звіту, *Norton Cyber Safety Insights Report* [160] у 2023 р. понад 595 млн дорослих людей стикалися з кіберзлочинністю, а 463 млн осіб заявили, що у 2022 р. стали особисто жертвами кібератак. При цьому понад 54% споживачів у всьому світі повідомили, що стикалися з кіберзлочинністю, а майже 2 з 5 респондентів стали жертвами у 2022 р. Середній показник втрат від кіберзлочинності становив близько 242 дол. США на особу. Крім того, кіберзлочинність завдала не лише фінансової шкоди, але й для усунення даних негативних наслідків жертви в середньому витратили 6,6 годин свого часу. Лідерами серед кіберзагроз стали шкідливе програмне забезпечення – 21%, виток даних – 15% та несанкціонований доступ до електронної пошти – 13%.

Ключовим елементом аналізу економічних наслідків кіберзлочинності є вивчення ролі індексів кібербезпеки, які характеризують оцінку готовності держави до протидії загрозам. Ці індекси враховують такі аспекти, як законодавча база, технічні засоби захисту, організаційні стратегії та міжнародне співробітництво. Дані свідчать, що країни з високими показниками кібербезпеки зазнають менших економічних витрат з тими, де рівень захисту залишається низьким. Необхідними інструментами для оцінки готовності країни до захисту даних в кіберпросторі в світі застосовуються наступні показники:

- Індекс розвитку інформаційно-комунікаційних технологій (*ICT Development Index, IDI*);
- Глобальний індекс кібербезпеки (GCI);
- Національний індекс кібербезпеки (NCSI);
- Національний індекс кіберпотужності (National Cyber Power Index, NCPI); Індекс розвитку ІКТ (IDI) – це всесвітньо визнаний показник, розроблений Міжнародним союзом електрозв’язку (ITU) для оцінки та порівняння розвитку інформаційно-комунікаційних технологій (ІКТ) у різних країнах. Він оцінює готовність до ІКТ, їх використання та навички, щоб отримати уявлення про цифровий розрив і технологічний прогрес у всьому світі [34].

На рис. 2.1. представлено показники Індексу розвитку інформаційно-комп’ютерних технологій у 2023 р. Лідерами рейтингу ІКТ у 2023 р. став Кувейт, Фінляндія та Естонія з показником 100, 98,1 та 97,9 відповідно. Найнижчий показник Індексу розвитку ІКТ зосереджено у ЧАД та становить 21,3.

Дані свідчать про значний розрив у рівнях розвитку інформаційно-комп'ютерних технологій між різними країнами світу. Високі показники, продемонстровані Кувейтом, Фінляндією та Естонією, пояснюються значними

інвестиціями в цифрову інфраструктуру, впровадженням інноваційних технологій та високим рівнем цифрової грамотності населення. З іншого боку, найнижчий показник, зафіксований у Чаді, демонструє серйозні обмеження в доступі до сучасних технологій, недостатнє фінансування сфери ІКТ і низький рівень освіти в галузі цифрових навичок. Такий дисбаланс підкреслює необхідність глобальних зусиль для зменшення цифрового розриву, зокрема через міжнародні програми підтримки, трансфер технологій та стимулювання розвитку цифрової грамотності

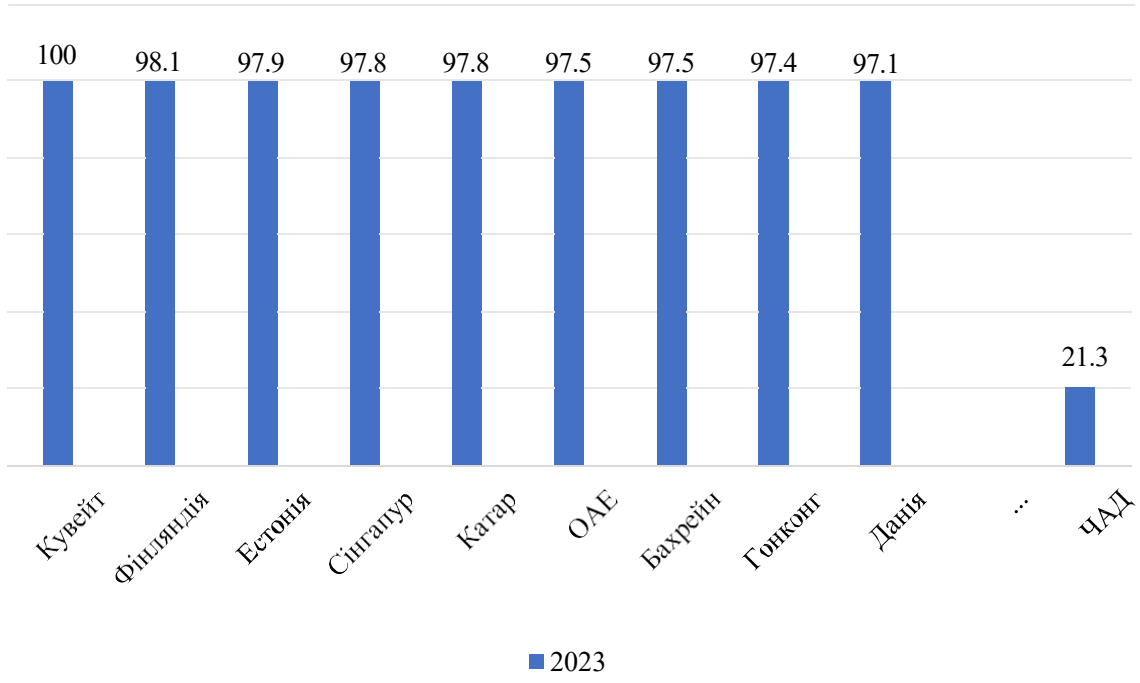

Рис. 2.1. Індекс розвитку інформаційно-комунікаційних технологій (IDI), 2023 р.

Джерело: побудовано автором на основі [19].

Дослідивши Глобальний індекс кібербезпеки можна зробити висновок, що у 2023 р. рейтинг очолили США, Італія, Велика Британія, Єгипет, Саудівська Аравія та Португалія, Корея з оцінкою 100 балів, відповідно зайнявши лідируючу першу позицію.

На рис. 2.2. представлено показник Глобального індексу у 2023 р.

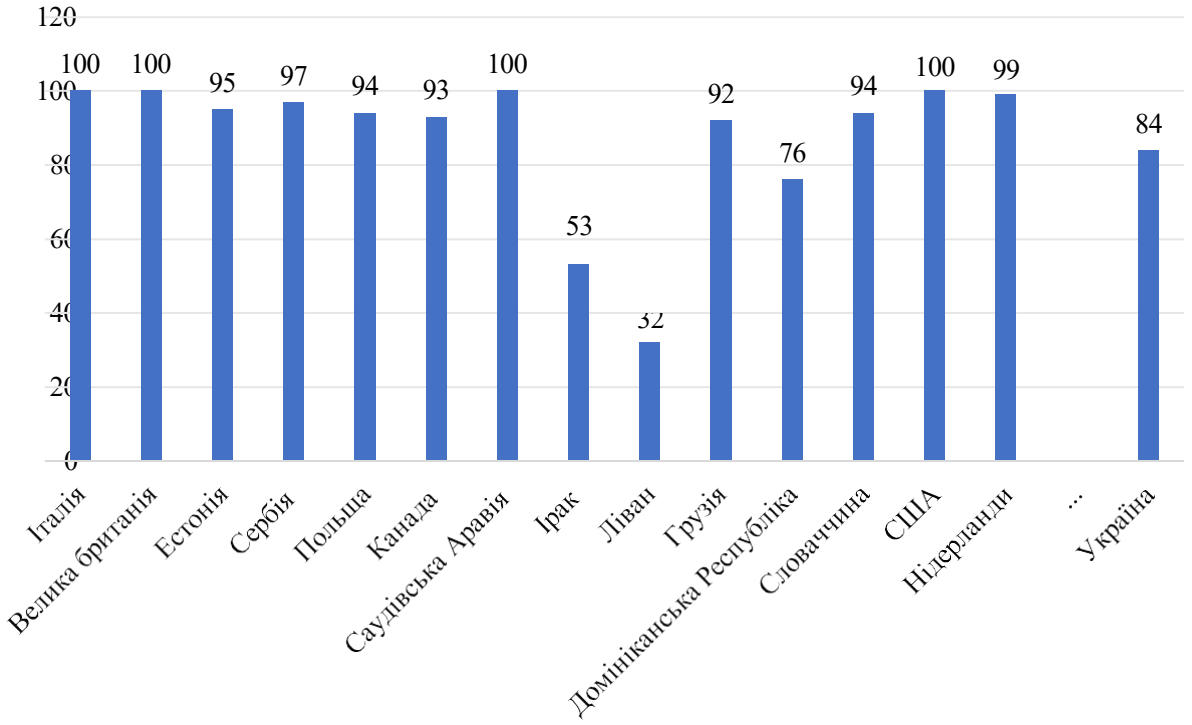

Рис. 2.2 Глобальний індекс кібербезпеки у світі (GCI), 2023 р.

Джерело: побудовано автором на основі [19].

Глобальний індекс кібербезпеки (*GCsI*) – це комплексний показник, який вимірює рівень кібербезпеки країни, розроблений за ініціативою ITU *Global Cy GCsI* розраховується з 2017 р. для 194 країн світу. Глобальний індекс кібербезпеки (*GCI*) дозволяє здійснити комплексну оцінку кібербезпеки всіх країн світу за п’ятьма складовими чинниками: а) юридичні (*legal measures*) – вимірювання законів і нормативних актів щодо кіберзлочинності та кібербезпеки; б) технічні (*technical measures*) – технічні можливості у сфері кібербезпеки; в)організаційної підготовленості (*organizational measures*) - вимірювання національних стратегій та організацій, які впроваджують кібербезпеку; г) розвитку освітнього та дослідницького потенціалу країни (*capacity development*) – наявність науково-дослідних, освітніх та підготовчих програм, а також сертифікованих фахівців та держустанов, що сприяють

нарощуванню потенціалу у сфері інформаційної безпеки; д) готовності до співпраці (cooperative measures) – вимірювання партнерства між агентствами, фірмами та країнами.

Аналіз за кількісними показниками з використанням складових критеріїв глобального індексу кібербезпеки дозволяє зазначити, що за критерієм організаційної підготовленості показник України (13,6) перевищує аналогічний показник Молдови (15,51). Позитивну ситуацію можна спостерігати й за показником розвитку освітнього та дослідницького потенціалу країни – показник України (14,61) перевищує аналогічний показник Молдови (8,04). За всіма іншими показниками спостерігається відставання від аналогічних показників сусідніх країн.

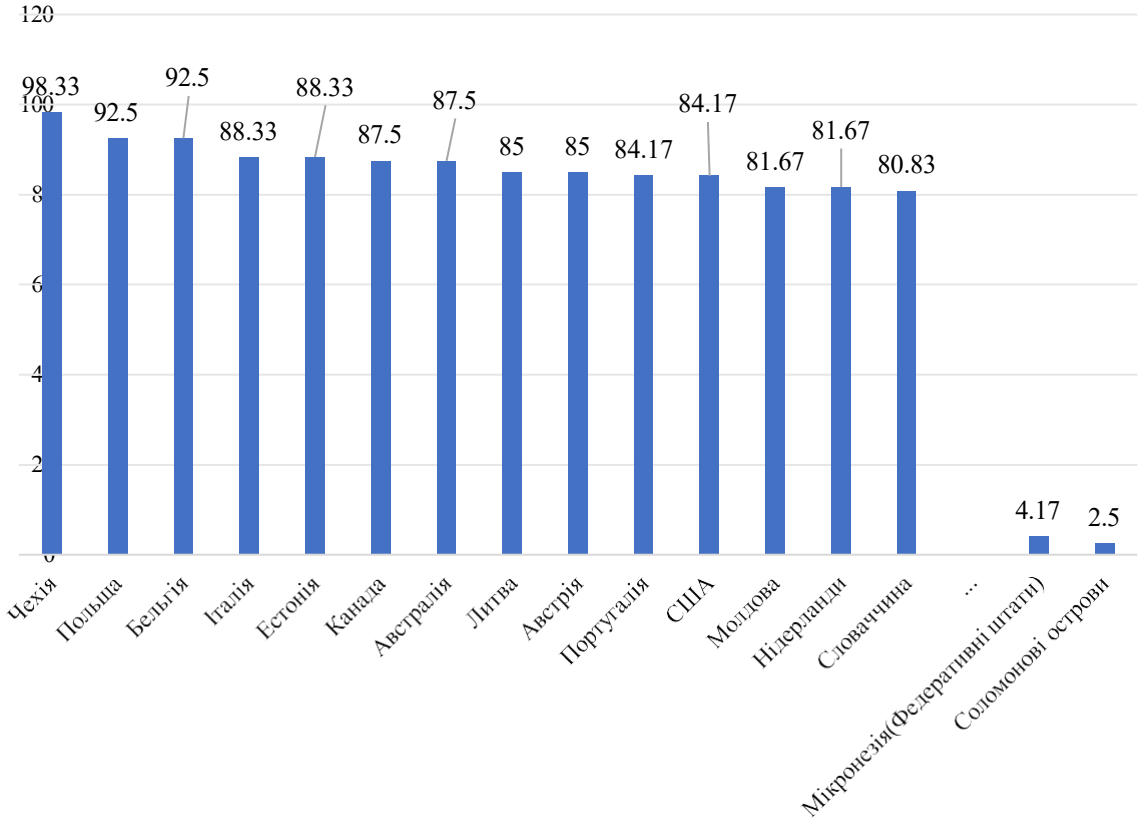

Рис. 2.3. Динаміка країн за Національним індексом кібербезпеки (NCSI) у 2023 р.

Національний індекс кібербезпеки (*NCSI*), який запропоновано проєктною групою Академії електронного урядування м. Таллінн, Естонія

[16]. Динаміку NCSI України та її позиціонування відносно інших країн світу наведено на рис. 2.3.

Індекс базується на чотирьох ключових категоріях, які охоплюють різноманітні аспекти кіберзахисту, таких як: законодавча база – нормативно-правові акти, положення, накази тощо; організаційна інфраструктура, яка забезпечує кібербезпеку – існуючі організації, відділи тощо; формати співпраці – комітети, робочі групи тощо; результати – політика, вправи, технології, вебсайти, програми тощо. Оцінка NCSI показує, який відсоток країна отримала від максимального значення показників. Оцінка індексу демонструє, наскільки країна наблизилася до максимально можливого рівня ефективності у впровадженні заходів кібербезпеки. Кінцева оцінка виражається у відсотках, де максимальний бал становить 100 (або 100%).

Чехія посіла перше місце серед представлкних країн в рейтингу показника Національного індекса кібербезпеки у 2023 році, показник дорівнює близько98,33% зі 100 можливих, на другому місці зосереджена Польща та Бельгія з показником 92,5%. На третьому місці знаходиться Італія та її показник становить 88,33% Лідерство Чехії зумовлено сильними нормативними ініціативами та надійною кіберінфраструктурою. Цифровий розвиток також демонструє стабільний прогрес, хоч і менший, ніж кібербезпека. Найменші показники серед досліджених країн зосереджено у Мікронезії та Соломонові острови. Дані свідчать про слабкість рівня кібербезпеки, обмежені урядові ініціативи та недосконалі стратегії захисту критичної інфраструктури.

Важливим показником разом з Національним індексом кібербезпеки є рівень цифрового розвитку (рис. 2.4), адже позитивна різниця між цими показниками свідчить про розвиток кібербезпеки країни знаходиться на досить високому рівні. Негативний результат показує, що цифрове суспільство країни є більш розвиненим, ніж національна сфера кібербезпеки. Даний

показник розраховується відповідно до Індексу розвитку електронного уряду (*EGDI*) та Індексу готовності до мереж (*NRI*). *DDL* – це середній відсоток, який країна отримала від максимального значення обох індексів [13].

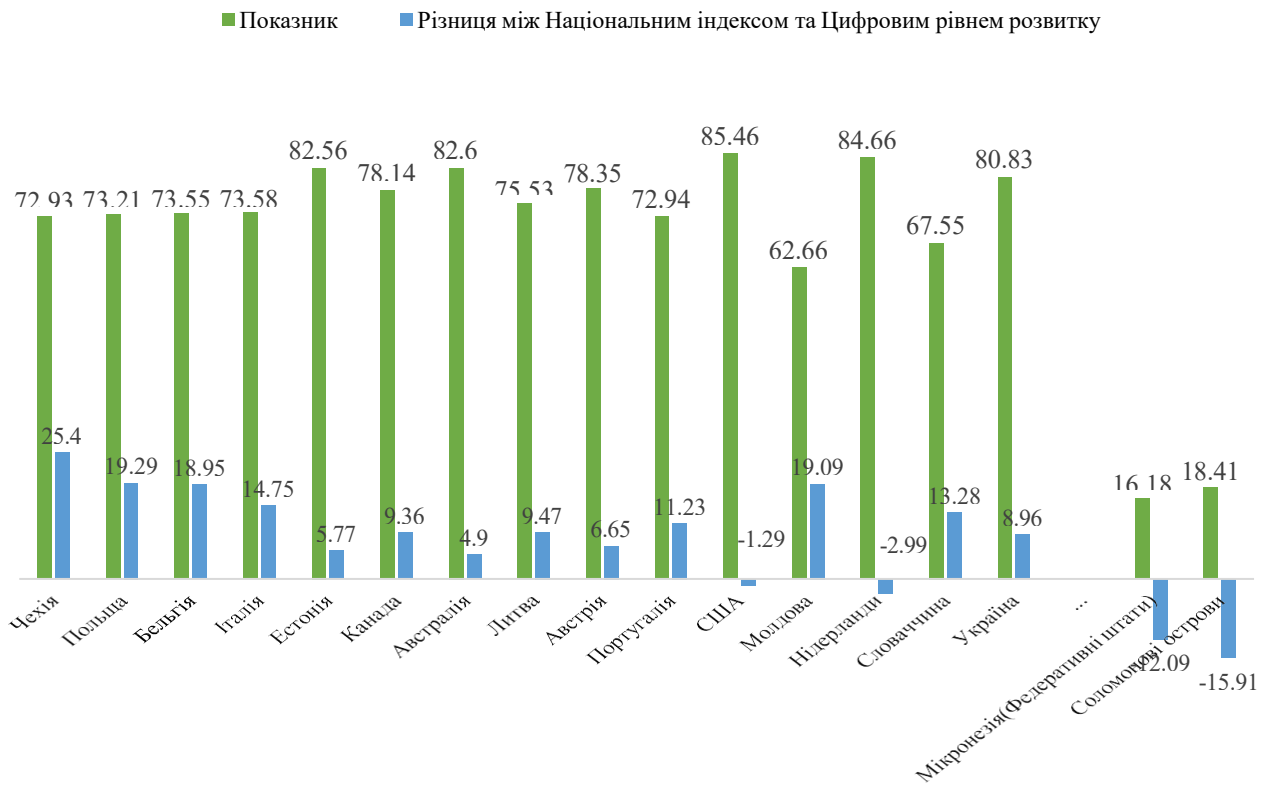

Рис. 2.4. Динаміка країн за цифровим рівнем розвитку у 2023 р.

Джерело: побудовано автором на основі [163].

США має незначний від'ємний баланс (-1,29) між показником та рівнем цифрового розвитку, це вказує що цифровий розвиток випереджає інвестиції у кібербезпеку. Китай теж має різницю – 17,94, цей розрив демонструє значну потребу в корисних заходах кібербезпеки. Країни з меншими розривами (наприклад, Чехія) демонструють більшу ефективність у використанні цифрових технологій без компромісів у безпеці.

Виконання індексу *NCSI* Україною передбачено наступними складовими:

- військовий кіберзахист – виконано на 100%. Даний показник надає інформацію чи мають збройні сили країни (або інші фінансовані урядом та

організовані військовими організаціями, яким доручено територіальну оборону) визначені організації, які пов’язані або з кібероперaціями, або з кібербезпекою військових операцій, з відповідними завданнями та мандатів;

- боротьба з кіберзлочинністю – виконано на 100%. Індикатор відстежує, чи криміналізовані національним законодавством наступні кіберзлочини: навмисний доступ без права до комп’ютерної системи (шляхом порушення заходів безпеки) (незаконний доступ); умисне перехоплення з використанням технічних засобів непублічної передачі комп’ютерних даних без права (незаконне перехоплення); навмисне пошкодження, видалення, погіршення, зміна або приховування комп’ютерних даних без права (втручання в дані); навмисне серйозне перешкоджання без права функціонування комп’ютерної системи шляхом введення, передачі, пошкодження, видалення, погіршення, зміни чи приховування комп’ютерних даних (системне втручання); та навмисне вчинення конкретних дій підготовчого характеру з використанням певних пристроїв або доступу до даних, які будуть використані для вчинення кіберзлочинів, згаданих вище (неправомірне використання пристроїв);

- кіберкризове управління виконано на 56% зі 100%. Індикатор вимірює наявність національного кризового плану для боротьби з широкомасштабними кібератаками, інцидентами або значними загрозами;

- реагування на кіберінцинденти – виконано на 64% зі 100 %. Індикатор відстежує наявність національного *CSIRT/CERT/CIRT* у країні. Згідно з визначенням Університету Карнегі-Меллона, NCSI визнає національними *CSIRT* ті *CERT*, які визначені країною чи економікою як відповідальні за кіберзахист країни чи економіки. Такі національні *CSIRT* можуть бути розташовані в уряді чи за його межами, але мають бути спеціально визнані урядом як такі, що мають загальнонаціональні повноваження та відповідальність;

- захист персональних даних – виконано на 100%. Показник відстежує наявність національного законодавства, яке встановлює принципи обробки даних, права особи (суб'єкта даних) щодо їхніх даних, а також зобов'язання та відповідальність контролерів і обробників даних;
- аналіз кіберзагроз та підвищення обізнаності – виконано на 75%. Даний показник оцінює спроможність і практику проведення оцінок кіберзагроз і тенденцій на національному рівні. Оцінки можуть, наприклад, складатися встановленою державною установою чи підрозділом (наприклад, департаментом чи агентством) або міжвідомчою спільною робочою групою;
- кібербезпека цифрових трансформацій – виконано на 83%. Даний показник є національно визнане рішення, яке дозволяє безпечно та надійно ідентифікувати осіб під час онлайн-транзакцій. Таке рішення повинно, як мінімум, бути доступним для взаємодії з організаціями державного сектору з можливістю застосування в приватному секторі;
- кібербезпека критичної інформаційної інфраструктури – виконано на 75%. Показник вимірює наявність законодавчо встановленої основи або

механізму для ідентифікації компонента інформаційної інфраструктури КІ або основних послуг;

- дослідження та розробка кібербезпеки – виконано на 100%. Показник вимірює участь уряду в дослідженнях і розробках у сфері кібербезпеки, що підтверджується офіційним визнанням та/або державним фінансуванням і підтримкою відповідної дослідницької програми;
- освіта та професійний розвиток – виконано на 60%. До сфери застосування цього показника входять компетенції з кібербезпеки в системі державної освіти, тобто найдоступнішій формі початкової освіти, доступній в країні;
- внесок у світову кібербезпеку – виконано на 67%. Цей показник оцінює готовність країни фінансувати, організовувати або іншим чином

сприяти проекту(ам) з розбудови потенціалу, спрямованому на конкретні країни або групу країн;

- політика кібербезпеки – виконано на 100%. Цей показник визначає, чи було офіційно покладено відповідальність за кібербезпеку на найвищий урядовий чи політичний рівень.

Невиконання деяких складових свідчить про необхідність вдосконалення національних кризових навчань щодо кібербезпеки та відсутність повної інтеграції до міжнародних кіберкризових навчань. Брак участі з міжнародними партнерами у спільних навчаннях з міжнародними партнерами знижує ефективність у протидії масштабними кіберзагрозами. Відсутність кадрів у сфері кібербезпеки збільшує ризики для загрози критичної інфраструктури та національної безпеки. Регулярні перевірки щодо кіберризиків відсутні або ж є неефективними на державному рівні що призводить до погіршення кіберкризового управління в цілому. Отже, проаналізувавши основні показники кіберзлочинності, можна зробити висновок, що зберігається тенденція щодо збільшення негативних фінансових наслідків від кіберзагроз. Необхідними заходами є впровадження комплексних і скоординованих заходів щодо загрози кіберзлочиннотсі на національному та міжнародному рівнях. Це забезпечить активну участь органів влади, бізнесу та суспільства для запобігання кіберінцидентам. На основі аналізу позицій України в міжнародних рейтингах кібербезпеки та вивчення індикаторів, що лежать на основі глобальних індексів *NCSI, GCI* та *NCPI*, визначено сильні та слабкі сторони кіберпроможності країни. До перспективних напрямків віднесено вдосконалення систем захисту інформації об’єктів критичної інфраструктури, спираючись на найкращі світові практики, а також координацію дій з міжнародними організаціями у протидії загрозам, що працюють в умовах розвитку цифрової економіки та інформатики.

2.2. Організаційно-функціональна характеристика Міністерства цифрової трансформації України

Міністерство цифрової трансформації України (Мінцифри) є ключовим суб'єктом державної політики у сфері цифровізації, що одночасно виступає як об'єкт та регулятор процесів, критичних для національної кібербезпеки. У зв'язку з цим, організаційно-функціональна характеристика діяльності Мінцифри є необхідною для визначення інституційних рамок впровадження інноваційних інструментів формування стратегії кібербезпеки. Далі буде розглянуто місію, структуру та ключові повноваження Міністерства, які безпосередньо корелюють із завданнями захисту цифрового суверенітету 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.

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 КМУ [13]. 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.

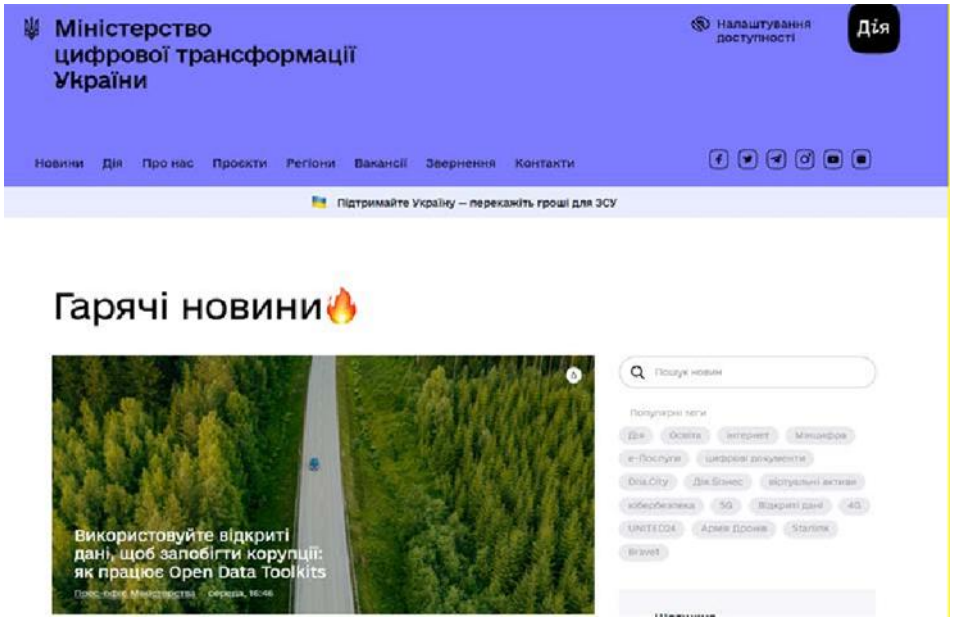

Рисунок 2.5 – Веб-сайт Міністерства цифрової трансформації України

Проведемо аналіз даних на офіційному сайті Міністерства цифрової трансформації України, результати якого на рис. 2.5 та 2.6. [16-19]

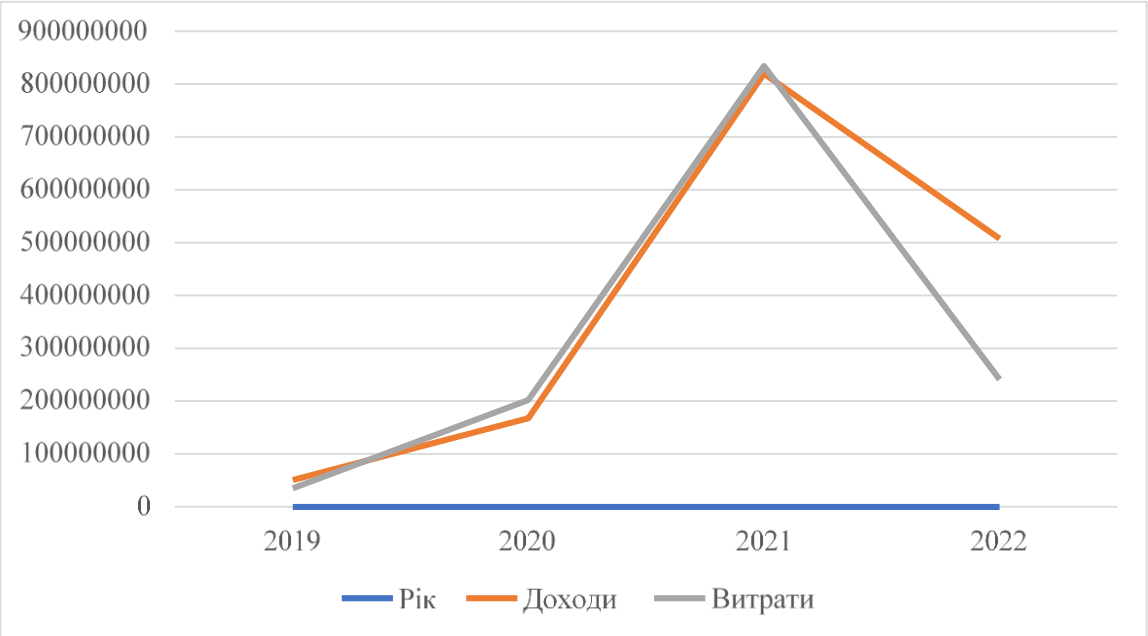

Рисунок 2.6 – Доходи та витрати фінансової діяльності Міністерства цифрової трансформації України за звітній період

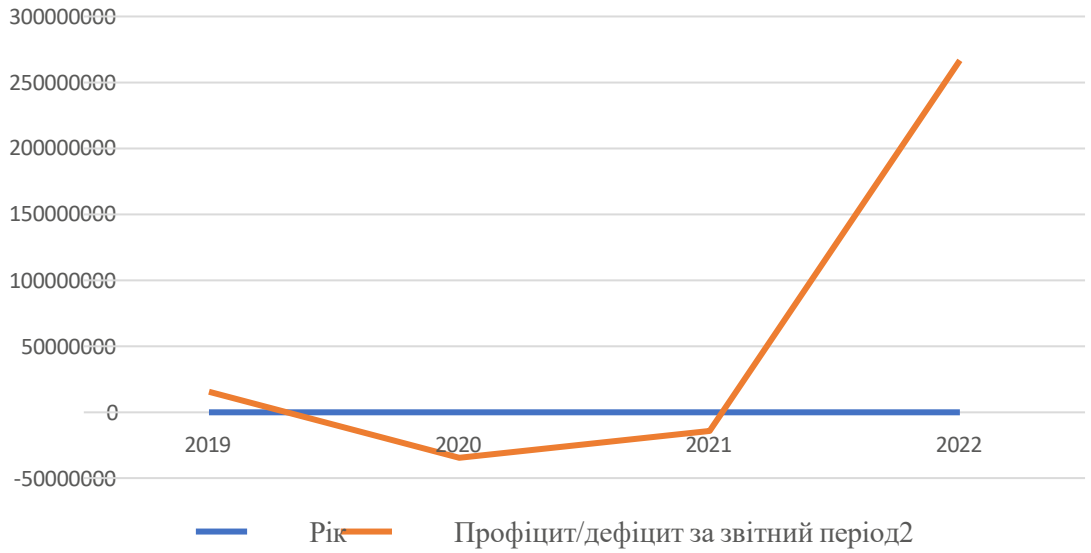

Рисунок 2.7 – Профіцит/дефіцит фінансової діяльності Міністерства цифрової трансформації України за звітній період

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 КМУ 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 Мінцифри до є: 1) забезпечення 100% доступність публічних послуг онлайн, тобто всі публічні послуги повинні бути доступні громадянам та бізнесу через інтернет без будь-яких перешкод; 2) забезпечення 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 матимуть доступ до швидкого Інтернету; 3) залучення 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) збільшення частки IT у ВВП країни до 10%: Це значить, що інформаційні технології стануть більшим фактором у валовому внутрішньому продукті країни. [48]

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. 2.8).

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.

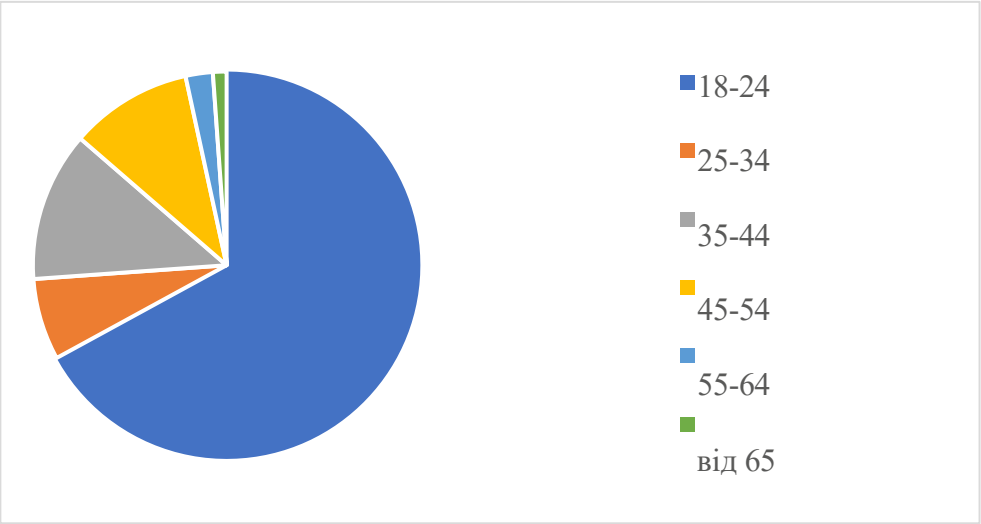

Рисунок 2.8 – Розподіл відношення до цифрової ідентифікації за віковими групами

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.

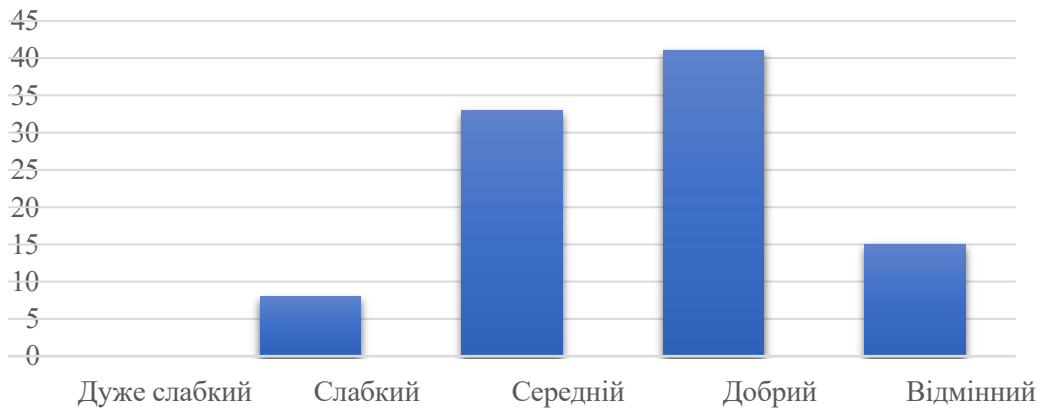

Рисунок 2.9 – Рівень інформованості щодо цифрової ідентифікації

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

Результати опитування на рис. 2.9 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.

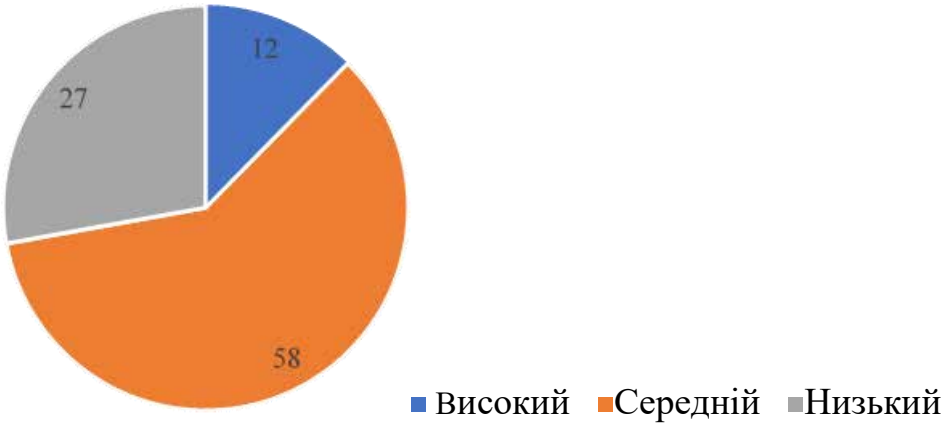

Рисунок 2.10 – Сприйняття про рівень загальної інформованості населення про цифрову ідентифікацію в Україні

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.

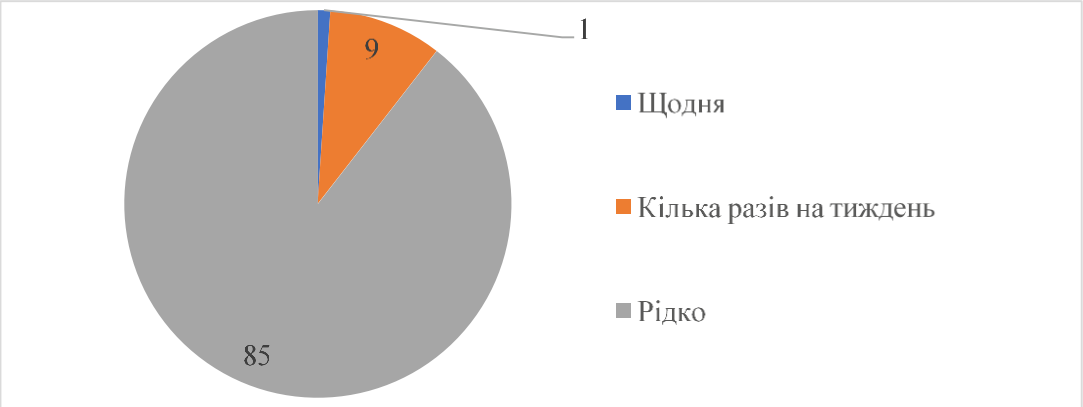

Рисунок 2.11 – Частота прочитання новин або статей про цифрову ідентифікацію

У розгляді участі в навчальних заходах чи інформаційних кампаніях (рис. 2.12), 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.

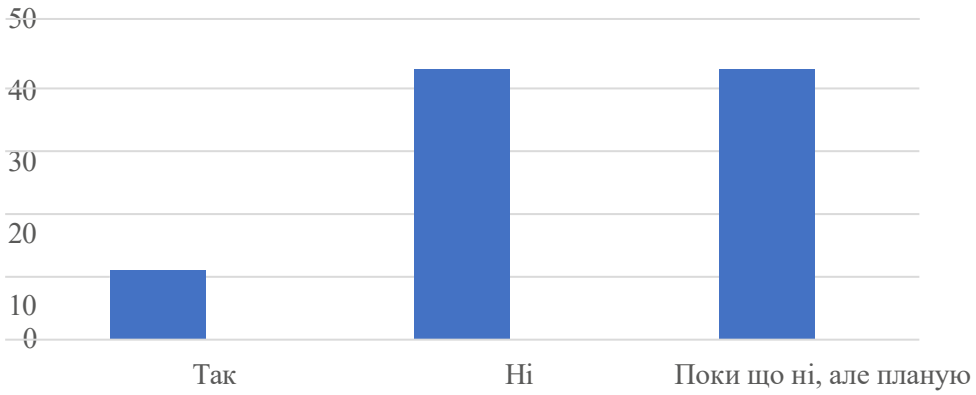

Рисунок 2.12 – Участь у навчальних заходах чи інформаційних кампаніях, що стосуються цифрової ідентифікації

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 населенняЗа результатами дослідження (рис. 2.13) найпопулярніші джерела отримання інформації про цифрову ідентифікацію визначено як новинні сайти, офіційні джерела (урядові та корпоративні веб-сайти) та соціальні мережі.

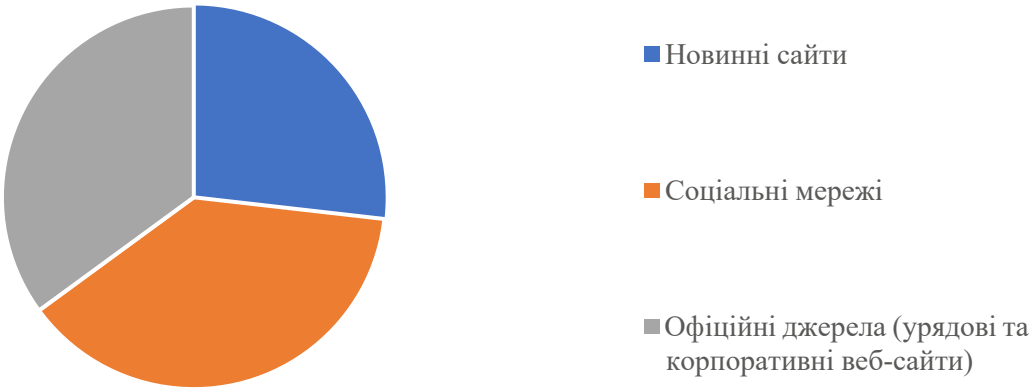

Рисунок 2.13 – Найпопулярніші джерела отримання інформації про цифрову ідентифікацію

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.

Внаслідок аналізу відповідей (рис. 2.14) 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

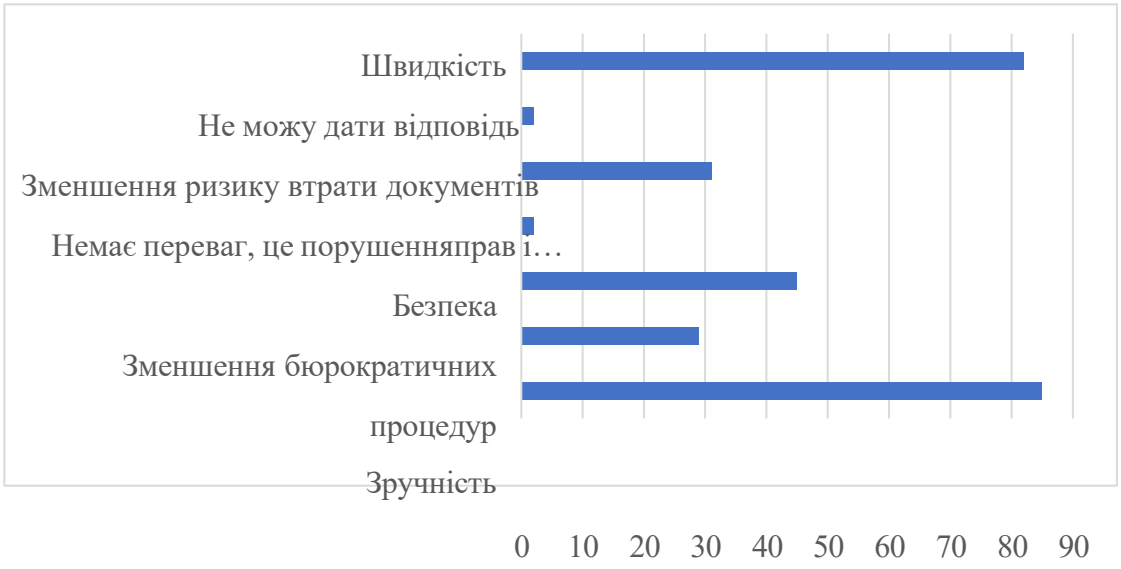

Рисунок 2.14 – Основні переваги у використанні цифрової ідентифікації

Аналізуючи основні недоліки 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.

Стосовно ставлення до конфіденційності особистих даних при використанні цифрової ідентифікації (рисунок 2.15), виділяється кілька ключових позицій.

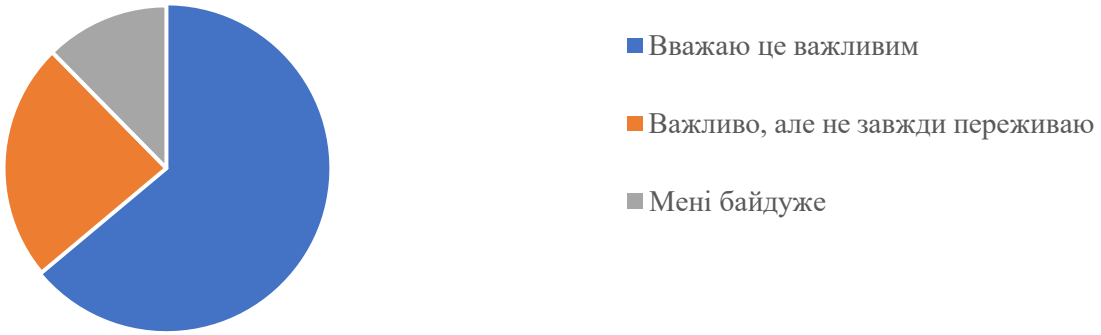

Рисунок 2.15 – Ставлення до конфіденційності особистих даних при використанні цифрової ідентифікації

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.

Стосовно довіри до організацій та платформ, які зберігають особисті дані при цифровій ідентифікації (рис. 2.16), 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 2.16 – Довіра організаціям та платформам, які зберігають особисті дані при цифровій ідентифікації

Розподіл рівня інформованості щодо заходів безпеки на платформах цифрової ідентифікації (рисунок 2.17) 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

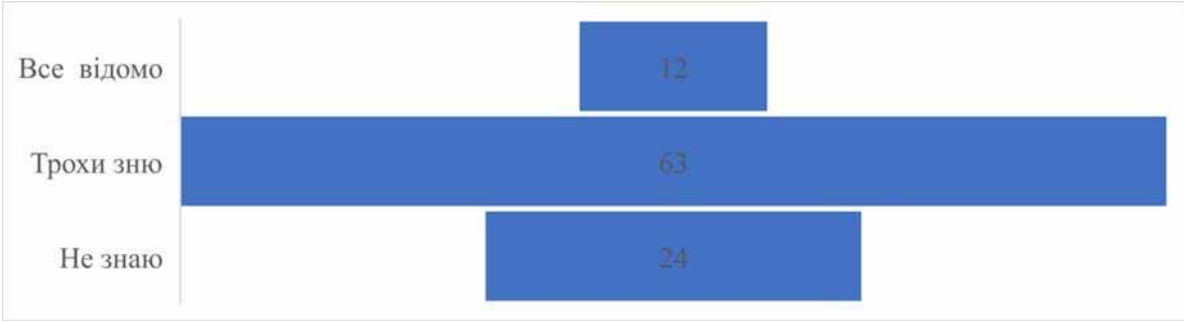

Рисунок 2.17– Проінформованість про заходи безпеки для захисту даних на платформах цифрової ідентифікації

Щодо використання двофакторної аутентифікації 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

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.

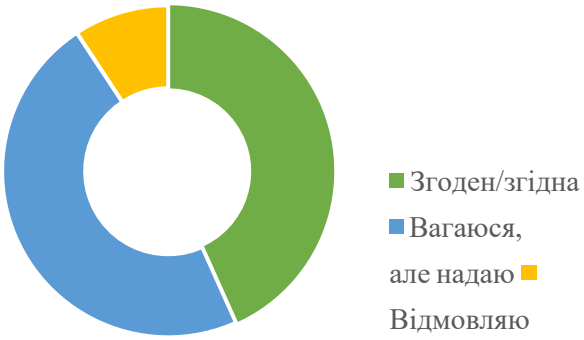

Рисунок 2.18 – Реакція на звернення на платформі цифрової ідентифікації для надання додаткових даних для підтвердження особи

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.

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.

Також виникає негативна реакція на повідомлення про можливий доступ третіх сторін до ваших даних на платформі цифрової ідентифікації (рис. 2.19).

Рисунок 2.19 – Думка щодо використання особистих даних без згоди користувача на платформах цифрової ідентифікації

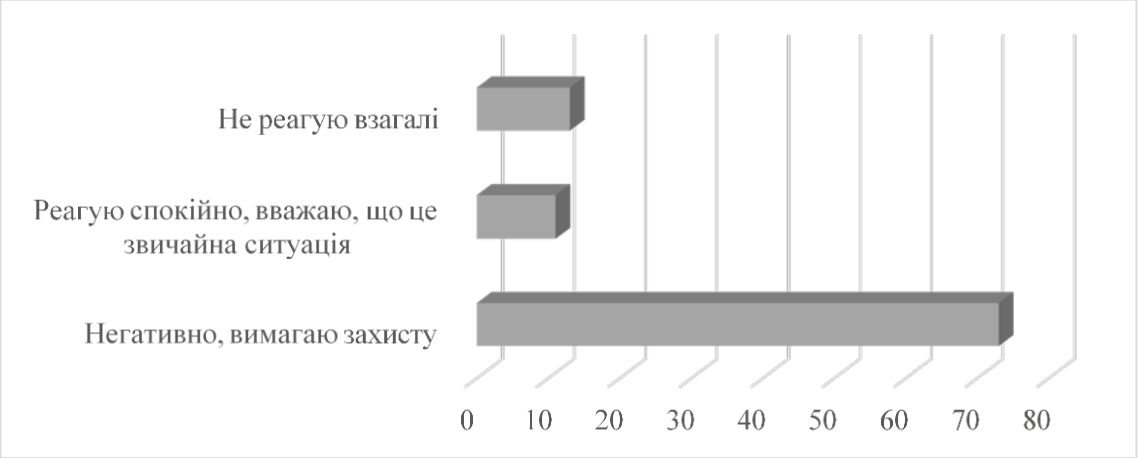

Рисунок 2.20 – Реакція на повідомлення про можливий доступ третіх сторін до ваших даних на платформі цифрової ідентифікації

Щодо знань про можливість скасування облікового запису на платформі цифрової ідентифікації при виникненні проблем можна виділити різний рівень знань серед учасників (рис. 2.21). 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.

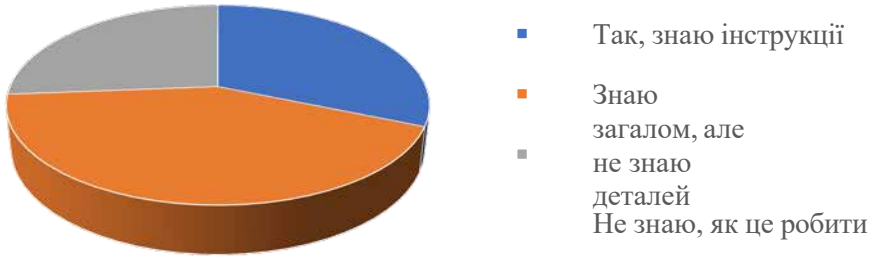

Рисунок 2.21 – Знання про скасування облікового запису на платформі цифрової ідентифікації при виникненні проблем

Згідно рис. 2.22 більшість користувачів вважає, що цифрова ідентифікація як спосіб підтвердження особи для доступу до послуг є зручною

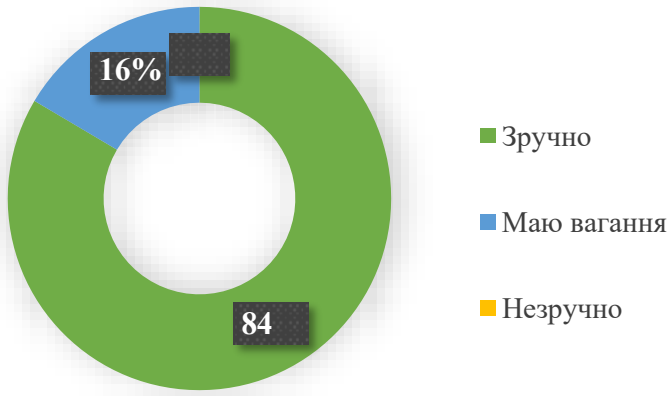

Рисунок 2.22 – Зручність цифрової ідентифікації як спосіб підтвердження особи для доступу до послуг

Щодо частоти використання цифрової ідентифікації у повсякденному житті відзначається різний рівень активності серед учасників (рис. 2.23). 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.

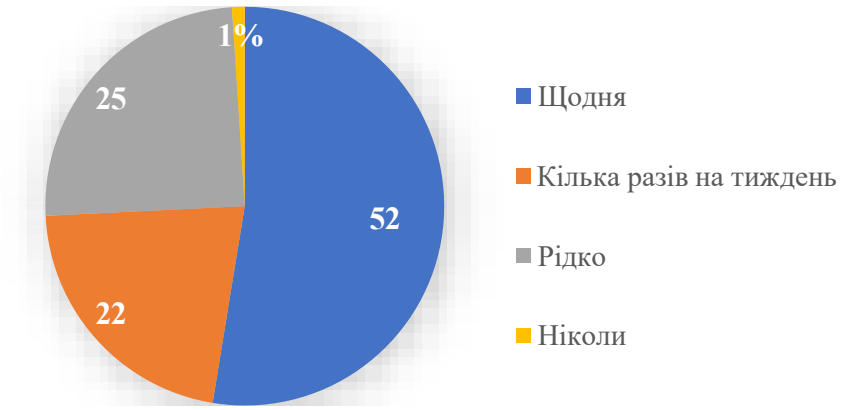

Рисунок 2.23– Частота використання цифрової ідентифікації у повсякденному житті

Незначна 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.

Більшість користувачів вважає, що цифрова ідентифікація допомагає запобігати шахрайству та кіберзлочинам (рис. 2.24).

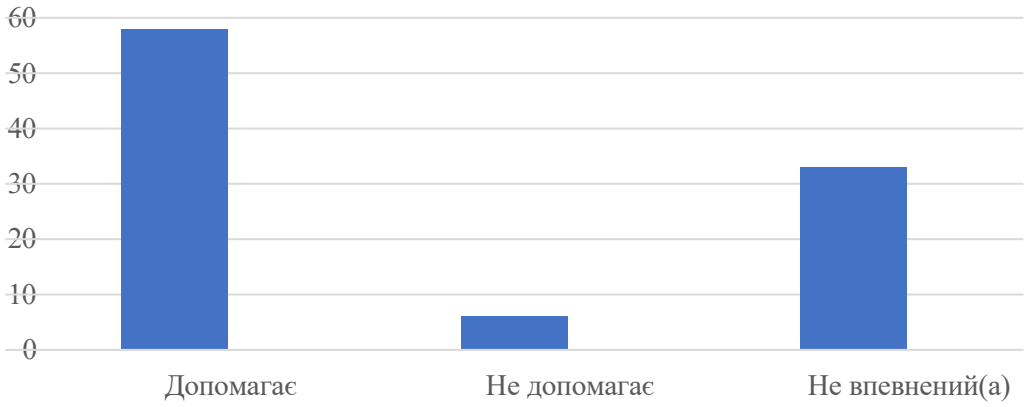

Рисунок 2.24 – Позиція респондентів щодо визнання цифрової ідентифікації як чинника у запобіганні шахрайства та кіберзлочинів

Майже всі погоджуються з тим, що цифрова ідентифікація важлива для розвитку цифрової трансформації України, тому у всіх опитуваних користувачів є в наявності смартфон з підтримкою функцій цифрової ідентифікації (рис. 2.25).

Рисунок 2.25 – 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.

Висновки до розділу 2.

1. Зазначено, що недостатня участь України разом з міжнародними партнерами у спільних навчаннях з подолання кібертероризму знижує

ефективність у протидії масштабними кіберзагрозами. Відсутність кадрів у сфері кібербезпеки збільшує ризики для загрози критичної інфраструктури та національної безпеки. Отже, проаналізувавши основні показники кіберзлочинності, можна зробити висновок, що зберігається тенденція щодо збільшення негативних фінансових наслідків від кіберзагроз.

2. Необхідними заходами є впровадження комплексних і скоординованих заходів щодо загрози кіберзлочиннотсі на національному та міжнародному рівнях. На основі аналізу позицій України в міжнародних рейтингах кібербезпеки та вивчення індикаторів, що лежать на основі глобальних індексів *NCSI, GCI* та *NCPI*, визначено сильні та слабкі сторони кіберпроможності країни. До перспективних напрямків віднесено вдосконалення систем захисту інформації об’єктів критичної інфраструктури, спираючись на найкращі світові практики, а також координацію дій з міжнародними організаціями у протидії загрозам, що працюють в умовах розвитку цифрової економіки та інформатики.

3. Обґрунтувано роль цифрової ідентифікації, як ключового фактора забезпечення кібербезпеки та основи для встановлення довіри в публічному управлінні, що вказує на необхідність створення основи для ефективної та безпечної взаємодії громадян, бізнесу та влади 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. УДОСКОНАЛЕННЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ НА ОСНОВІ РОЗВИТКУ СИСТЕМИ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ ТА ІННОВАЦІЙНИХ ПІДХОДІВ

3.1. Забезпечення конфіденційності та безпеки даних цифрової ідентифікації як стратегічний пріоритет кібербезпеки в публічному управлінні.

У відповідності до експертної думки, основними проблемами, у сучасному процесі цифрового розвитку України, є: 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., КМУ встановлено, 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 введеного 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 «ДІЯ», 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 «Дія». [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. Багатоаспектна роль цифрової ідентифікації у формуванні стратегії кібербезпеки: доступність, інтеграція та взаємодія суб'єктів.

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 ma 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) Цифрову стратегію Європейської Комісії: Перетворення Комісії в цифровоорієнтовану, спрямовану на користувачів та оптимізовану на основі даних; 2) Стратегію єдиного цифрового ринку для ЄС, яка спрямована на створення єдиного цифрового ринку в ЄС; 3) Формування цифрового майбутнього ЄС: Розвиток стратегії для цифрового майбутнього; 4) Білу книга з штучного інтелекту. Європейський підхід до досконалості і довіри: Визначення європейського підходу до розвитку штучного інтелекту; 5) Європейську стратегія щодо даних: Розробка стратегії для роботи з даними.; 6) План дій Європейської Комісії щодо 5G: Визначення заходів для розвитку мереж 5G; 7) Директиву 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) Стратегію 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 напрямах 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 розгорнут 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 даникса 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].

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.

3.3. Стратегічні ввввектори розвитку кібербезпеки на засадах інноаційних підходів

Чинна стратегія кібербезпеки України визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1]. Сьогодні кібербезпека є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Формуючи нову Стратегію кібербезпеки України, потрібно враховувати світові тренди в глобальному кіберсередовищі, як фактори впливу на розбудову національної системи кібербезпеки.

У зв’язку з появою нових системних загроз національній безпеці 21 червня 2018 р. було ухвалено новий Закон України «Про національну безпеку України» [2]., який відобразив сучасні безпекові реалії та стратегічні напрямки розвитку сектора безпеки України. Відповідно до п. 9 ч. 1 ст. 1 цього Закону національна безпека — це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних загроз. Складові частини національної безпеки наведено на рис. 3.2.

Рисунок 3.2. Структура національної безпеки України

За вказаними напрямами безпеки здійснюється планування. Документи, що містять довгострокові плани, отримали назву стратегії. Відповідно в законі описуються в загальному вигляді стратегії національної безпеки, воєнної безпеки, громадської безпеки та цивільного захисту України тощо. Окремим нормативним актом затверджено Стратегію кібербезпеки України [1] – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [3]. Докладніше структуру вказаного документа наведено на рис. 3.3.

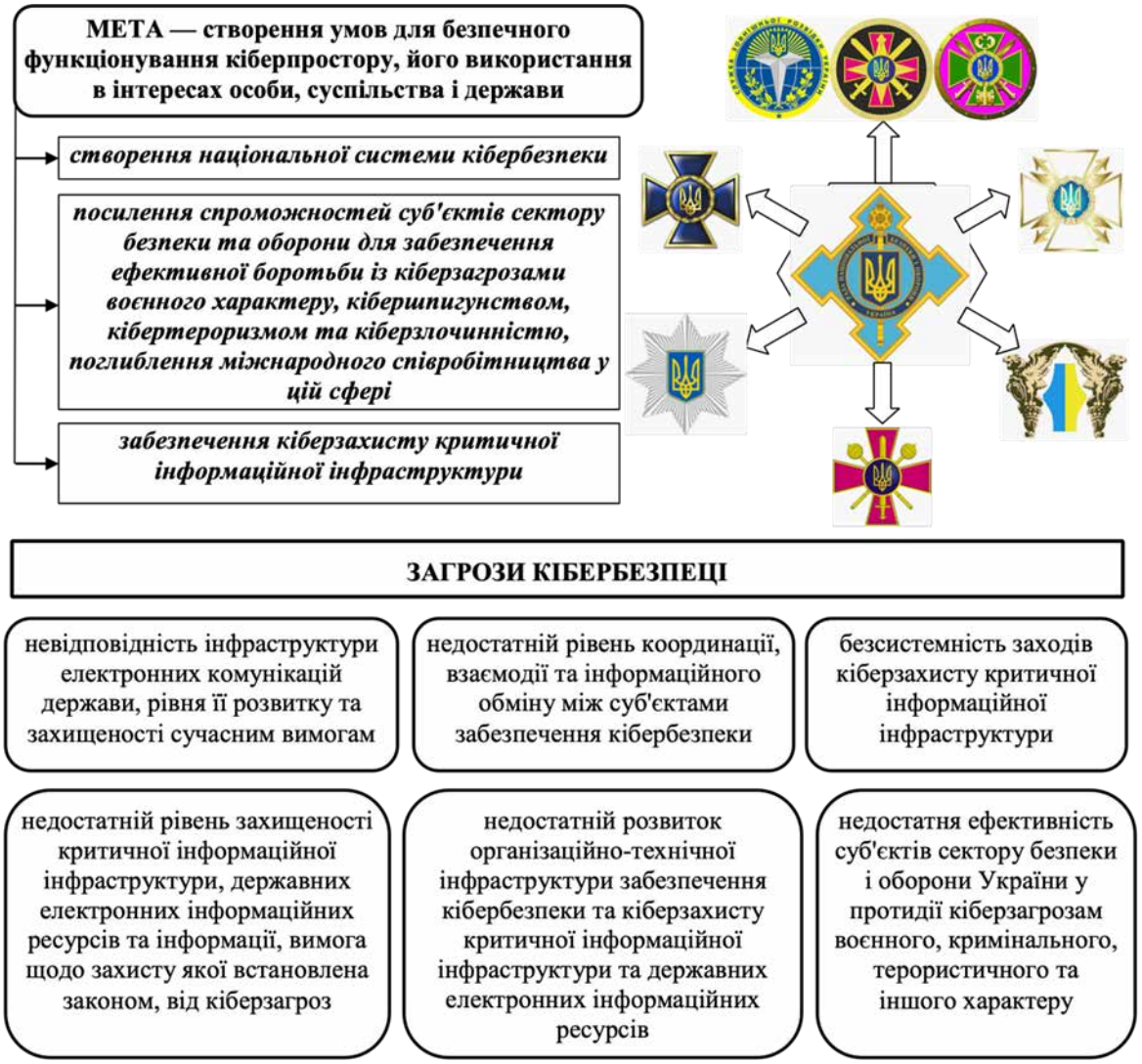

Рисунок 3.3. Основні елементи стратегії кібербезпеки України, розроблено автором на основі [3].

XXI століття знаменується активним формуванням шостого технологічного укладу (біо-, нано-, інфо-, когнотехнологій, їх конвергенцією) та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій, зокрема їх використання у кіберпросторі.

Питома вага кіберзагроз у сфері загроз національній безпеці країн змінюється, і ця тенденція в процесі розвитку інформаційних технологій таїх конвергенції з технологіями штучного інтелекту зростає. Посилення такого

впливу на функціонування структур управління як національних, так і транснаціональних формує повністю нову безпекову ситуацію з викликами нового технологічного рівня. Міжнародні центри сили зазнають перерозподілу сфер впливу у кіберпросторі, збільшується їх бажання через такий поділ забезпечити втілення власних геополітичних інтересів.

Структуру Національної системи забезпечення кібербезпеки у розрізі рівнів управління наведено на рис.3.4.

Рисунок 3.4. Національна система забезпечення кібербезпеки,

розроблено автором на основі [4].

Кіберпростір разом з іншими територіями визнано одним з потенційних театрів воєнних дій, тому здатність держави захищати свої національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили тенденція до створення нового типу військ – кібервійськ, до завдань яких входить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а також проведення превентивних наступальних операцій у кіберпросторі, спрямованих на ураження обчислювальних мереж та інформаційних систем збройних сил

Цифрова трансформація, яка є одним із пріоритетів розвитку України, створює нові виклики у сфері кібербезпеки. Впровадження нових технологій та цифрових послуг вимагає системного підходу до кібербезпеки та оцінки ризиків. Без цього існує ризик втрати довіри громадян до процесів цифрової трансформації.

Сучасні світові тренди в розвитку кібербезпекового середовища створюють різноманітні виклики для України, які виявляються у внутрішніхпроцесах та явищах країни. Одним із головних джерел загроз є активне використання кіберпростору в гібридній агресії з боку Росії. Росія відома своєю активною кіберагресією проти України, спрямованою на деструктивний вплив на органи державної влади, системи управління військами, а також на об’єкти критичної інфраструктури. Ця діяльність включає в себе розвідувальні операції, кібершпигунство та кібердиверсії, які мають серйозний потенціал для завдання шкоди Україні. Також зростає загроза кібертероризму, що пов'язано з кіберможливостями Росії та використанням кіберпростору для фінансування терористичних груп. Недостатня взаємодія з міжнародними партнерами у сфері кібербезпеки ускладнює боротьбу з цією загрозою У зв'язку з цим, Україні необхідно посилити свої зусилля у напрямку кібербезпеки, зокрема шляхом нарощування кіберзахисту критично важливих об'єктів інфраструктури, збільшення співпраці з міжнародними партнерами та розвитку власних кіберзбройних сил. Таким чином можна ефективно протистояти сучасним кіберзагрозам та забезпечити безпеку та стабільність в кіберпросторі. Для ефективної боротьби з цими загрозами Україні потрібно вдосконалити законодавство, забезпечити належний рівень кіберзахисту на всіх рівнях та підвищити кіберграмотність населення. Також важливо підвищити фінансування робіт з кіберзахисту та підвищити рівень кваліфікації фахівців у цій галузі.

Забезпечення кібербезпеки для України стає вельми важливим у контексті сучасних глобальних викликів, оскільки цифрова інфраструктура є критичним компонентом національної безпеки. Визначення пріоритету забезпечення кібербезпеки допомагає запобігти серйозним загрозам для державних інформаційних ресурсів, промислових систем, та особистих даних громадян.

Стратегічні цілі забезпечення кібербезпеки включають розвиток ефективної системи захисту від кібератак, підвищення кіберграмотності населення та розвиток кадрового потенціалу у цій сфері. Постійна модернізація та удосконалення кіберзахисту є стратегічним завданням для забезпечення стійкості інформаційних систем та захисту національних інтересів. Забезпечення кібербезпеки є не лише національним пріоритетом, але й ключовою умовою для стабільного розвитку держави та її інтеграції у сучасний цифровий світ.

Сьогодні пріоритетами забезпечення кібербезпеки України є по- перше, убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки, а по-друге, формування нової якості національної системи кібербезпеки, що потребує чіткого та зрозумілого визначення стратегічних цілей, які мають бути досягнуті протягом періоду реалізації Стратегії.

Для формування потенціалу стримування (С) при розбудові національної системи кібербезпеки на основі стримування, кіберстійкості та сприянню взаємодії до 2026 року держава повинна досягти стратегічних цілей.

Для досягнення дієвої кібероборони (ціль С.1) Україна має не лише створити та розвивати ефективні (у тому числі кадрово та технологічно) підрозділи з повноваженнями ведення збройного протиборства в кіберпросторі, але й сформувати належну правову, організаційну,

технологічну модель їх функціонування та застосування, що неможливо без: ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належного навчання та фінансового забезпечення таких структур, систематичного проведення кібернавчань, оцінки спроможностей та ефективності підрозділів, розроблення та імплементації індикаторів оцінки їх діяльності [1]. Для посилення спроможностей у протидії розвідувально-підривній діяльності у кіберпросторі та кібертероризму (ціль С.2.) Україна забезпечить безперервне здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів держави, суспільства і окремих громадян.

З метою посилення спроможностей у протидії кіберзлочинності (ціль С.3.) правоохоронні та державні органи спеціального призначення з правоохоронними функціями набудуть спроможностей для мінімізації загроз кіберзлочинності, посилять свій технологічний і кадровий потенціал для проведення превентивних заходів та розслідування кіберзлочинів.

В процесі розвитку асиметричних інструментів стримування (ціль С.4.) потрібно створити необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу неурядового сектору [1].

Для набуття кіберстійкості (К) при розбудові національної системи кібербезпеки на основі стримування, кіберстійкості та сприянню взаємодії до 2026 року держава повинна досягти стратегічних цілей, З метою посилення національної кіберготовності та кіберзахисту (ціль К.1.) потрібно запровадити та реалізовувати чіткі та зрозумілі для всіх стейкхолдерів заходи з посилення

національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав та свобод кожного українського громадянина. Кіберготовність полягає у здатності всіх стейкхолдерів, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявлення та усунення передумов до їх виникнення, забезпечивши тим самим кіберстійкість, насамперед об’єктів критичної інформаційної інфраструктури.

В процесі підвищення професійного вдосконалення, розбудови кіберобізнаного суспільства та розвитку науково-технічного забезпечення кібербезпеки (ціль К.2.) виникає потреба у проведенні докорінної реформи системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки. Забезпеченні збереження наявного кваліфікованого кадрового потенціалу суб’єктів кібербезпеки. Стимулюванні дослідження і розробки у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів, створенні національних інформаційних систем, платформ і продуктів. Вітчизняний науково-технічний потенціал першочергово залучатиметься до вирішення завдань забезпечення кібербезпеки держави. Кібергігієна, цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним мають стати невід’ємними елементами освіти кожного українського громадянина

Для забезпечення безпечних цифрових послуг (ціль К.3) виникає потреба у досягненні балансу між потребами українського суспільства, вітчизняного ринку, економіки держави та необхідністю забезпечити безпеку в кіберпросторі; забезпеченні надійностіта безпеки цифрових послуг з моменту створення та протягом усього їхнього життєвого циклу.

Для набуття взаємодії (В) при розбудові національної системи кібербезпеки на основі стримування, кіберстійкості та сприянні взаємодії до 2026 року держава повинна досягти стратегічних цілей. З метою зміцнення

системи координації (ціль В.1.) держава повинна створити умови для ефективної взаємодії суб'єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки, а також для результативних спільних дій під час попередження, відбиття та нейтралізації наслідків кібератак та кіберінцидентів. Також виникає потреба у координації діяльності усіх стейкхолдерів задля подолання кризових ситуацій у кібербезпеці.

Для формування нової моделі відносин у сфері кібербезпеки (ціль В.2.) виникає потреба у запровадженні сервісної моделі державної участі у заходах з кіберзахисту, за якої держава сприйматиметься не як джерело вимог, а як партнер у розбудові національної системи кібербезпеки [1, 3].

Для забезпечення прагматичного міжнародного співробітництва (ціль В.3.) відносини з міжнародними партнерами потрібно спрямувати як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками.

Посилення спроможностей національної системи кібербезпеки здійснюється шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей. Цей процес є ключовим завданням у забезпеченні національної безпеки, який досягається шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей.

Стратегічні завдання, орієнтовані на підвищення рівня готовності до кібернападів, включають у себе не лише підвищення свідомості громадськості про кібербезпеку, але й забезпечення підвищення кваліфікації фахівців з кібербезпеки та розвиток відповідних кадрових ресурсів. Важливими аспектами посилення системи кібербезпеки є також постійна

модернізація та удосконалення її, що сприяє запобіганню кіберзлочинності та захисту особистих даних громадян. Зокрема, підвищення обізнаності громадськості щодо кібербезпеки сприяє зниженню ризиків та підвищує загальний рівень захищеності, що в свою чергу є ключовим фактором для забезпечення національної безпеки та стабільності держави.

Головним зовнішньополітичним пріоритетом України у сфері кібербезпеки має бути зміцнення євроінтеграційних процесів шляхом уніфікації підходів, практик і засобів забезпечення кібербезпеки з усталеними стандартами ЄС і НАТО, вжиття інших затверджених із стратегічними іноземними партнерами заходів, спрямованих на підвищення кіберстійкості України, розвиток можливостей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Україна повинна приділяти увагу спільній з партнерами протидії міжнародному тероризму, виявленню, попередженню і припиненню злочинів проти миру і безпеки людства, іншим протиправним діям, що порушують міжнародний правопорядок та інтереси демократичної світової спільноти, заснованню на договірній основі з партнерськими спецслужбами країн-членів ЄС і НАТО взаємовигідному обміну інформацією та досвідом щодо забезпечення національної безпеки у кіберпросторі, використанню кращих світових практик, активно здійснювати інші спільні заходи, що сприятимуть розвитку наукової, матеріально-технічної бази та кадрового потенціалу у сфері кібербезпеки.

Україна повинна співпрацювати з міжнародними партнерами, організаціями та іншими заінтересованими сторонами, які поділяють спільне бачення майбутнього кіберпростору як глобального, відкритого, вільного, стабільного та безпечного, в основі якого дотримання прав людини, основних свобод та демократичних цінностей, які гарантують соціально-економічний та політичний розвиток України. Наша держава має продовжувати активну

участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН, а також добровільних необов'язкових норм, правил та принципів відповідальної поведінки держави. Це потребуватиме більшої координації та консолідації заінтересованих сторін на міжнародних форумах, в яких Україна має бути не лише учасником, але й ініціатором та організатором.

Виходячи з того, що Інтернет давно став суспільним надбанням, істотно вийшов за межі суто національних інтересів, наша держава повинна максимально сприяти мультистейкходерській (багатосторонній) моделі управління Інтернетом, підтримуючи міжнародні, регіональні та національні дискусії з цього питання, сприяючи залученню до цього процесу приватного сектору, наукових та освітніх кіл, громадянського суспільства. Україна сприятиме подальшому дотриманню міжнародного права та стандартів у галузі прав людини, заохочуватиме застосування найкращих практик, а також активізує свої зусилля щодо запобігання зловживанню новими технологіями. Для цього держава повинна підвищити участь і партнерство в міжнародних процесах стандартизації та сертифікації у сфері кібербезпеки, розширити представництво в міжнародних, регіональних та інших органах стандартизації, організаціях, що займаються розробленням стандартів та сертифікацією у цій сфері.

У питаннях розроблення стандартів у сферах нових технологій (зокрема щодо штучного інтелекту, хмарних технологій, квантових обчислень та квантових комунікацій) та базової архітектури Інтернету Україна повинна дотримуватись позиції, що Інтернет повинен лишатися глобальним та відкритим, технології мають спрямовуватися на людину, забезпечувати її базові свободи, гарантувати невтручання у її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження в цій частині мають

здійснюватися лише відповідно до закону. Використання технологій має бути законним, безпечним та етичним.

Враховуючи взаємопов'язаність сучасного кіберпростору та з метою розвитку співпраці між державою, приватним сектором економіки, науковими і освітніми колами та громадянським суспільством у сфері кібербезпеки, Україна повинна вдосконалювати національний кіберпростір як глобальний, відкритий, вільний, стабільний і, перш за все, безпечний, що є гарантією успішного розвитку країни.

В процесі реалізації Стратегії [1, 4-5, 7] Україна повинна зробити кібербезпеку одним з основних питань своєї міжнародної діяльності, посилюючи для цього потенціал своїх зовнішньополітичних структур та кіберпотенціал держави. З цією метою Україна має розвивати мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва. Процес реалізації Стратегії має бути максимально прозорим, відкритим та супроводжуватися демократичним цивільним контролем.

Першочерговим завданням для України є розроблення та запровадження індикаторів стану кібербезпеки на основі системного моніторингу виявлення і прогнозування кіберзагроз, що надасть змогу фіксувати досягнення або недоліки функціонування системи кібербезпеки.

Крім того, важливим напрямом є розроблення інтегральної системи оцінювання новітніх технологій, що безпосередньо мають вплив на кіберстійкість держави, створення інструментів (стандарти, протоколи, сертифікати тощо) з оцінювання ефективності використання новітніх технологій з протидії кібератакам. Ефективність реалізації Стратегії повинна визначатися через постійний моніторинг її виконання та спиратися на чітку систему розроблених індикаторів стану кібербезпеки. Індикатори мають визначати прогрес, якого досягли суб'єкти забезпечення кібербезпеки в

реалізації Стратегії з таких питань, як: виконання стратегічних Завдань у межах цілей (в розрізі завдань); досягнення стратегічних цілей (в розрізі цілей); ступінь впливу заходів, що здійснюються, на національну систем кібербезпеки та цифрову трансформацію держави.

Запровадження індикаторів стану кібербезпеки забезпечить покращення процес моніторингу виконання Стратегії кібербезпеки у реальному часі з використанням сучасних веб-ресурсів (онлайн-платформ), прозорість вжитих заходів для суспільства та держави. Посилення впливу національної системи кібербезпеки на суспільний розвиток буде визначатися за визначеними критеріями: підвищення рівня довіри населення до держави щодо безпечності кіберпростору; формування безпечного інформаційного суспільства, в якому до заходів кібербезпеки крім державних інституцій залучені приватні суб'єкти та громадяни; позитивний вплив на захист національних інтересів у сфері кібербезпеки (як приклад, рівень впливу на розвиток ситуації, пов'язаної з агресією російської федерації проти України).

За допомогою розгалуженої системи індикаторів визначатиметься стан досягнення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Система індикаторів повинна включати базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що дасть можливість комплексно оцінювати результативність та ефективність реалізації Стратегії кібербезпеки.

Визначені концептуальні підходи до подальшого розвитку національної системи кібербезпеки базуються на: 1) загальному розумінні та аналізі кіберсередовища, світових кібертрендів (з урахуванням національних

особливостей), незаперечному захисті національних інтересів України; 2) стійкості у вдосконаленні законодавства у галузі кібербезпеки; 3) спрямованості на економічний і соціальний прогрес суспільства; 4) забезпеченні балансу між потребами держави і правами громадян, додержанні законності, процесуальних гарантій та засобів правового захисту; 5) чіткому визначенні ролей, потреб і обов'язків при вирішенні завдань кібербезпеки на різній складності рівні; 6) орієнтації на ризики при забезпеченні кібербезпеки та кіберзахисту; 7) впровадженні механізмів партнерства між державним і приватним сектором у галузі кібербезпеки; 8) активному підході, який передбачає проведення запобіжних заходів; 9) забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки.

Метою реалізації Стратегії кібербезпеки України на 2025–2030 роки [1] є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави. Документ ґрунтується на засадах стримування, кіберстійкості та взаємодії.

Отже, в процесі підготовки магістерської роботи розглянуто сутність та значення інформаційної безпеки держави, а також проаналізовано основні кіберзагрози, досліджено Стратегію кібербезпеки України, її цілі, завдання та основні положення, проведено оцінювання впливу Стратегії кібербезпеки України на забезпечення інформаційної безпеки держави, а також будуть вироблено пропозиції щодо її вдосконалення.

Висновки до розділу 3.

1.Високий рівень безпеки особистих даних, можливо досягти 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.

2. Вказано, що 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.

3. Доведено, що для того, щоб навчити користувачів і працівників органів публічної влади перевагам та безпеці цифрової ідентифікації, освіта та навчання мають стати важливим компонентом вказаного процесу з акцентуванням на співпрацю з освітніми установами. Успішне впровадження та функціонування системи цифрової ідентифікації побудовано на такій співпраці. Це дозволяє залучати різні стейкхолдерів та забезпечити оптимальний розвиток системи, який допомагає громадянам і загальному суспільству.

3. У процесі підготовки магістерської роботи розглянуто сутність та значення інформаційної безпеки держави, а також проаналізовано основні кіберзагрози, досліджено Стратегію кібербезпеки України, її цілі, завдання та основні положення, проведено оцінювання впливу Стратегії кібербезпеки України на забезпечення інформаційної безпеки держави, а також будуть вироблено пропозиції щодо її вдосконалення

ВИСНОВКИ

У магістерській кваліфікаційній роботі «Інноваційні інструменти формування стратегій кібербезпеки органів держвної влади» доведено, що кібербезпека в державному секторі є стратегічною функцією публічного управління, що виходить за межі суто технічного захисту. Вона спрямована на забезпечення національної кіберстійкості, недоторканності критичної інформаційної інфраструктури та цілісності державних електронних реєстрів.

Результати даного магістерського дослідження на тему, «Інноваційні інструменти формування стратегій кібербезпеки органів держвної влади», а також реалізовані мета й завдання дають підстави сформувати такі висновки та рекомендації.

1. Уточнено сутність, зміст принципів та стратегічної функцію кібербезпеки в системі державного управління. Поняття «кібербезпека» у вітчизняних наукових джерелах розглядається, як багатокомпонентне та динамічне, зокрема: як стан захищеності життєво важливих інтересів особи, суспільства та держави у кіберпросторі, пов’язаний із запобіганням та нейтралізацією цифрових загроз; як діяльність або сукупність технічних та організаційних заходів, спрямованих на захист інформаційних систем, мереж і даних від атак та несанкціонованого доступу. Досліджено, що окремі автори включають до змісту поняття інформаційно-психологічний та управлінський виміри, розглядаючи кібербезпеку, як здатність протидіяти негативному впливу й забезпечувати цілісність інформаційних процесів. У наукових напрацюваннях вітчизняних і зарубіжних вчених простежується розуміння змісту кібербезпеки як елемента або підсистеми інформаційної безпеки, що є значно обємнішим поняттям. Узагальнення дозволяє визначити, що кібербезпека охоплює три ключові аспекти: стан захищеності, процес/діяльність із забезпечення захисту, система суб’єктів, методів і засобів.

Відповідно, варто зазначити, що кібербезпека постає як комплексна категорія, що поєднує технічні, правові й організаційні механізми та є важливою складовою національної безпеки України.

2. Проаналізовано функції ключових суб'єктів у сфері протидії кібертерозму та доведено, що на основі інституційних положеннь державного управління в сфері протидії кіберзлочинам, варто сформувати інституційний механізм, у складі якого: Президент України здійснює організаційну, інституційну, безпекову, захисну функції; ВРУ – організаційну, інституційну, безпекову, захисну, контрольну функції; РНБО, Державна служба спеціального зв’язку та захисту інформації – прогностично-планову, організаційну, інституційну, безпекову, захисну, контрольну функції; КМУ – прогностично-планову, керівну, організаційну, інституційну, безпекову, інформаційну, економічну; Державне бюро кібербезпеки, Національна поліція України, СБУ, ДБР – прогностично-планову, керівну, організаційну, контрольну, інституційну, діяльнісну, захисну, безпекову, інформаційну, економічну, правову функції; МЗС України та Міністерство культури та стратегічних комунікацій України – прогностично-планову, організаційну, контрольну функції тощо.

3. Обґрунтувана роль цифрової ідентифікації, як ключового фактора забезпечення кібербезпеки та основи для встановлення довіри в публічному управлінні, що впливає на різні аспекти публічного управління та сприяє його цифровій трансформації. Цифрова ідентифікація забезпечує ефективність, безпеку та відкритість органів публічної влади, полегшуючи їх взаємодію з громадянами та покращуючи якість наданих послуг. Акцентовано, що цифрова ідентифікація не обмежується лише технічними аспектами. Вона пов'язана з публічним контролем, прозорістю та громадською участю у владних процесах. 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.

4. На основі аналізу кращих зарубіжних практик таких країн, як: Естонія, Швеція, Сингапур, Канада, Бельгія, австрія загальнено, що серед основних факторів, які впливають на процес цифровізації державного управління та цифрової трансформації суспільства в зарубіжних країнах, варто виділити такі чинники, як: особливості ринкової економіки, які проявляють себе у збільшенні свободи підприємництва, вільний рух робочої сили та конкурентності на ринку праці; розвиток громадянського суспільства та соціального партнерства в цифровому середовищі; децентралізацію влади та впровадження ефективних структурних і регіональних політик.

5. Здійснено оцінку поточного впливу Стратегії кібербезпеки України на забезпечення інформаційної безпеки держави та виявити основні прогалини;

Розглянуто сутність та значення інформаційної безпеки держави, а також проаналізовано основні кіберзагрози, досліджено Стратегію кібербезпеки України, її цілі, завдання та основні положення, проведено оцінювання впливу Стратегії кібербезпеки України на забезпечення інформаційної безпеки держави, а також будуть вироблено пропозиції щодо її вдосконалення.

Дослідження дозволило визначити роль та місце Стратегії кібербезпеки України у системі забезпечення інформаційної безпеки держави, оцінити

ефективність Стратегії кібербезпеки України, розробити пропозиції щодо вдосконалення Стратегії кібербезпеки України. Результати дослідження можуть бути використані для вдосконалення Стратегії кібербезпеки України, а також для розроблення та впровадження інших заходів, спрямованих на посилення інформаційної безпеки держави.

6. Сформулювано пріоритети забезпечення конфіденційності та безпеки даних цифрової ідентифікації в публічному управлінні, що включає: підвищення рівня обізнаності серед населення щодо правил та безпеки використання цифрової ідентифікації може бути досягнуте через організацію кампаній та освітніх програм; забезпечення ефективної взаємодії та сумісність різних систем цифрової ідентифікації шляхом розробки стандартів, оскільки відповідність їм забезпечує захист особистих даних та конфіденційності є ключовим завданням і повинен ефективно забезпечувати безпеку громадянських даних від несанкціонованого доступу; здійснення регулярної перевірки та аудиту системи цифрової ідентифікації, що мають стати обов'язковими етапами для виявлення потенційних вразливостей та помилок; залучення громадськості в процес розробки та удосконалення системи цифрової ідентифікації; налагодження співпраці з приватним сектором може виявитися дієвим засобом для створення нових інноваційних продуктів в цілому контексті систем цифрової ідентифікації. 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: №984_011 від 27.06.2014 URL: 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, № 984_001-20 від 11.02.2020. URL: 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 ВРУ, 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 ВРУ № 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 ВРУ №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 ВРУ № 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 ВРУ 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 КМУ 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 КМУ 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 КМУ 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 КМУ 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 КМУ 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 05.05.2023URL: 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. URL: http://www.pag-journal.iei.od.ua/archives/2022/30-2022/8.pdf.

24. Ганущин С. Н. Імплементація 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. URL: 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/1Wp6IaHb0uRKb68mgebq8CvZbg BxupkCz

29. Карпенко О. В., Карпенко Ю. В. Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансферти: *Державне управління: удосконалення тарозвиток*. 2021. № 10. URL: 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.

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

36. Павлишин З. Я. Реформа системи впровадження сучасних технологій інформаційного забезпечення державного управління: *Інвестиції: практика та досвід*. 2019. № 2. URL: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.

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

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

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

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/Econom