ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПЕТРА МОГИЛИ

Кваліфікаційна наукова праця
на правах рукопису

АТАНАСОВ Микола Віталійович

УДК 35.088.6:004.738.5(043.3)

ДИСЕРТАЦІЯ

УПРАВЛІННЯ ПЕРСОНАЛОМ НА ДЕРЖАВНІЙ СЛУЖБІ У ВИМІРАХ ВЗАЄМОДІЇ В КІБЕРПРОСТОРІ

Спеціальність 281 «Публічне управління та адміністрування»
Галузь знань 28 «Публічне управління та адміністрування»

Подається на здобуття наукового ступеня
доктора філософії у галузі публічного управління та адміністрування

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

М. В. Атанасов

Науковий керівник: Ємельянов Володимир Михайлович, доктор наук з державного управління, професор.

МИКОЛАЇВ – 2025

АНОТАЦІЯ

Атанасов М. В. **Управління персоналом на державній службі у вимірах взаємодії в кіберпросторі**. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування». – Чорноморський національний університет імені Петра Могили, Миколаїв, 2025.

У дисертації здійснено науково-теоретичне обґрунтування та розроблено практичні рекомендації щодо підвищення ефективності управління персоналом на державній службі, обумовлених особливостями взаємодії в кіберпросторі, що дає підстави зробити відповідні висновки та узагальнення.

У першому розділі дисертації – *Концептуальні засади управління персоналом на державній службі у вимірах взаємодії в кіберпросторі* – проаналізовано ґенезис феномену «кіберпростір» з акцентом уваги на термінологічному значенні понять «взаємодії» та «ризики віртуального середовища»; описано базові механізми взаємодії державних службовців у кіберпросторі; виявлено парадигмальні зсуви в управління персоналом на державній службі в умовах розвитку інформаційного суспільства.

Комплексний аналіз наукової літератури, нормативно-правових документів з теми дисертації довів, що не існує єдиної, цілісної і всеохоплюючої теорії, яка пояснювала б усі аспекти управління персоналом на державній службі у вимірах взаємодії в кіберпросторі.

Запропонована концептуальна модель управління персоналом на державній службі у вимірах взаємодії в кіберпросторі концентрує дослідницьку увагу на описі ключових термінів, понять, визначень предметної області, а також теоретичних підходів, моделей, методів, інструментів щодо її аналізу. Кіберпростір трактується як простір функціонування продуктів

інформаційно-комунікаційних технологій, що дозволяють створювати складні системи взаємодій агентів (суб'єкти взаємодії) з метою отримання інформації, обміном та управління нею, а також здійснення комунікацій в умовах великої кількості мереж.

Констатовано, що кіберпростір має трьохвимірну структуру, складовими якої є фізичні, інформаційні та соціальні компоненти. Особливості взаємодії в кіберпросторі обумовлені феноменами «кіберпсихологічна готовність», «кібербезпека», «кіберзахист», «кібергігієна».

Доведено, що ризики в кіберпросторі охоплюють широкий спектр загроз як для організації (фінансові збитки, порушення конфіденційності даних, втрати репутації тощо), так і окремих осіб (порушення психічного здоров'я, професійне вигорання і т. ін.). Управління ризиками взаємодії в кіберпросторі повинна стани стрижнем HR-стратегій органів публічної влади.

Обґрунтовано, що базовими механізмами взаємодії державних службовців у кіберпросторі є: організаційно-правовий, інформаційно-технічний, соціально-психологічний. Саме через призму розуміння функціонування цих механізмів можна оцінювати ефективність взаємодії державних службовців у кіберпросторі, а також удосконалювати (модернізувати) таку взаємодію, під впливом зовнішніх та внутрішніх факторів.

Підкреслено, що основними передумовами парадигмальних зсувів в управлінні персоналом на державній службі є: цифровізація державного сектору; корпоративна та особиста кібербезпека державних службовців; взаємодія масмедіа та державної влади. Саме вони генерують необхідність впровадження комплексних змін у систему державної служби України, зокрема:

– обґрунтування концептуальних засад професійної діяльності державних службовців у кіберпросторі;

– впровадження нової компетентнісної моделі професійної діяльності державних службовців у кіберпросторі;

– модернізація технологій оцінювання готовності кандидатів на зайняття посад державної служби до здійснення професійної діяльності в умовах цифрового урядування та розвитку інформаційного суспільства;

– формування уявлень, цінностей і переконань про те, що цифрова компетентність, професійна мобільність, корпоративна та особиста кібербезпека стають стрижнем кар'єрного розвитку державних службовців.

У другому розділі – *Стан проблем професійної діяльності державних службовців у кіберпросторі* – охарактеризовано стан готовності державних службовців до професійної діяльності в кіберпросторі та визначено чинники, що впливають на професійну діяльність державних службовців у кіберпросторі.

Встановлено, що професійна активність державних службовців у цифровому середовищі супроводжується як новими можливостями для ефективної комунікації, так і зростанням соціальних ризиків, насамперед – кіберзалякуванням, кіберхейтом, прокрастинацією та цифровою втомою.

Опитування підтвердило, що значна частина державних службовців регулярно перебуває в інтернет-просторі не лише з професійною, а й з особистою метою. Водночас понад 40% з них зізналися у щоденному відволіканні на неслужбові онлайн-активності, а майже 22% постійно відкладають виконання службових завдань на користь другорядного цифрового контенту. Це вказує на поширення діджитал-прокрастинації як деструктивного чинника, що знижує продуктивність та ускладнює самоменеджмент державного службовця.

Однією з найгостріших проблем виявилося поширення кіберхейту – зневажливих висловлювань, принижень і ворожих дій у соціальних мережах, месенджерах, чатах і навіть у приватних повідомленнях. Кіберхейт часто стосується політичних тем, зовнішності, соціального статусу, гендеру і т. ін. Більшість респондентів визнають, що ці прояви викликають сильну емоційну реакцію: злість, засмучення, тривожність, що ускладнює збереження психологічної стійкості під час професійного функціонування.

Встановлено, що крему загрозу становить не лише переживання кібернасильства, а й участь самих державних службовців в агресивних діях у кіберпросторі. Значна частина респондентів зізналася у поширенні образливого контенту, що є показником цифрової незрілості, низької етичної стійкості та потреби в нормативній регуляції поведінки в мережі.

Виявлено також низький рівень інституційної довіри: респонденти не готові звертатися до керівництва, поліції чи психологічних служб у випадку кіберконфлікту, натомість переважно покладаються на неформальні джерела підтримки – друзів, родину або ні на кого. Це свідчить про потребу створення механізмів внутрішньої підтримки, підвищення довіри до служб безпеки та розвитку психологічної компетентності. Серед запитів на підтримку переважають освітні (тренінги, інформаційні ресурси), технічні (блокування, налаштування безпеки) та юридичні потреби. Це вказує на важливість формування інституційних програм цифрової обізнаності та професійної підготовки в контексті кібербезпеки.

Доведено, що професійна діяльність державних службовців у кіберпросторі детермінується сукупністю чинників: індивідуально-психологічних, соціально-комунікативних та організаційно-інституційних. Їх врахування є критично необхідним для формування цілісної системи цифрової адаптації та безпеки державної служби в умовах сучасних викликів.

У третьому розділі – *Шляхи удосконалення взаємодії державних службовців у кіберпросторі* – розглянуто можливість імплементація кращих міжнародних практик з удосконалення взаємодії державних службовців у кіберпросторі; напрямів та методів розвитку кіберпсихологічної компетентності державних службовців; проведення пропедевтичних заходів щодо попередження кібербулінгу та кіберхейту в системі державної служби України.

У розділі представлено адаптовану модель імплементації кращих міжнародних практик щодо взаємодії державних службовців у кіберпросторі. Виокремлено успішні підходи Нідерландів, Великої Британії, Канади,

Болгарії, Індії, Естонії, а також досвід Сінгапуру та Данії, де механізми «м'якого підштовхування» реалізуються через тонкі інтервенції у формі самопідказок у цифровому та організаційному просторах, використанні соціальних норм як підсилювачів відповідальності, а також застосуванні сенсорних сигналів (колір, структура документа), що підвищують ймовірність позитивної поведінкової реакції. Ефективність таких інтервенцій підтверджується результатами рандомізованих контрольованих експериментів (RCT), що дозволяють кількісно вимірювати поведінкові зміни, пов'язані із запровадженням конкретних інформаційних форматів або повідомлень.

Логічним продовженням імплементації міжнародного досвіду став розвиток кіберпсихологічної компетентності державних службовців як ключової умови підвищення їхньої цифровоповедінкової зрілості. Визначено її структуру (когнітивний, емоційнорегулятивний, поведінковий, етичний компоненти), проаналізовано виявлені вразливості (низька стресостійкість, схильність до реактивної агресії, відсутність навичок протидії кібербулінгу). Запропоновано поетапну систему формування цієї компетентності через навчальні модулі, роботу HR-психологів, інтерактивні симуляції та моніторинг показників цифрової поведінки. Розроблено матрицю індикаторів для оцінювання рівня компетентності, що поєднує кількісні та якісні методи. Вимірювання цифровоповедінкової зрілості інтегрується у кадрову політику як інструмент забезпечення безпечного, етичного та психологічно стійкого цифрового середовища.

Також у розділі розкрито пропедевтику кібербулінгу та кіберхейту як складову цифрової безпеки кадрової політики. Визначено основні форми цифрової агресії, причини її поширення у держсекторі та проаналізовано ризики для ефективності роботи колективу (зниження довіри, вигорання, деструкція комунікаційних зв'язків). Запропоновано науково обґрунтовані моделі інституційних механізмів реагування, що передбачають створення протоколів дій, відповідальних HR-підрозділів, цифрових омбудсменів, а

також реалізацію комунікаційних кампаній нульової толерантності до цифрової агресії з використанням освітніх платформ, чат-ботів та анонімних форм повідомлення.

Ключові слова: публічне управління, професійна компетентність публічних службовців, електронне урядування, державна служба, управління персоналом на державній службі, кіберпростір, кібербезпека.

ABSTRACT

Atanasov M. V. **Human resource management in public service in terms of interaction in cyberspace. – Qualification scientific paper. – Manuscript.**

Dissertation for the degree of Doctor of Philosophy in specialty 281 «Public management and administration» field of knowledge 28 «Public management and administration» Petro Mohyla Black Sea National University. Mykolaiv, 2025.

The dissertation provides a scientific and theoretical justification and develops practical recommendations for improving the effectiveness of personnel management in the civil service, determined by the peculiarities of interaction in cyberspace, which gives grounds for making appropriate conclusions and generalisations.

The first chapter of the dissertation, «*Conceptual Foundations of Personnel Management in the Civil Service in Terms of Interaction in Cyberspace»*, analyses the genesis of the phenomenon of 'cyberspace' with a focus on the terminological meaning of the concepts of "interaction" and 'risks of the virtual environment'; describes the basic mechanisms of interaction between civil servants in cyberspace; identifies paradigm shifts in human resource management in the civil service in the context of the development of the information society.

A comprehensive analysis of scientific literature and regulatory documents on the topic of the dissertation has shown that there is no single, comprehensive and all-encompassing theory that would explain all aspects of personnel management in the civil service in terms of interaction in cyberspace.

The proposed conceptual model of personnel management in the civil service in terms of interaction in cyberspace focuses research attention on the description of key terms, concepts, definitions of the subject area, as well as theoretical approaches, models, methods and tools for its analysis. Cyberspace is interpreted as the space in which information and communication technology products operate, allowing the creation of complex systems of interaction between agents (subjects of interaction)

for the purpose of obtaining, exchanging and managing information, as well as communicating in conditions of a large number of networks.

It has been established that cyberspace has a three-dimensional structure, consisting of physical, informational and social components. The peculiarities of interaction in cyberspace are determined by the phenomena of «cyberpsychological readiness», «cybersecurity», «cyberdefence» and «cyberhygiene».

It has been proven that risks in cyberspace cover a wide range of threats both for organisations (financial losses, data breaches, loss of reputation, etc.) and individuals (mental health problems, professional burnout, etc.). Managing the risks of interaction in cyberspace should be at the core of public authorities' HR strategies.

It has been established that the basic mechanisms of interaction between civil servants in cyberspace are organisational and legal, informational and technical, and socio-psychological. It is through the prism of understanding the functioning of these mechanisms that the effectiveness of interaction between civil servants in cyberspace can be assessed and such interaction can be improved (modernised) under the influence of external and internal factors.

It is emphasised that the main prerequisites for paradigm shifts in human resource management in the civil service are: the digitalisation of the public sector; corporate and personal cybersecurity of civil servants; interaction between the mass media and public authorities. These factors generate the need for comprehensive changes in the Ukrainian civil service system, in particular:

- justification of the conceptual foundations of the professional activities of civil servants in cyberspace;

- introduction of a new competency-based model of professional activities of civil servants in cyberspace;

- modernisation of technologies for assessing the readiness of candidates for civil service positions to carry out professional activities in the context of digital governance and the development of the information society;

- shaping perceptions, values and beliefs that digital competence, professional mobility, corporate and personal cybersecurity are becoming the backbone of civil servants' career development.

The second section, «*The State of Professional Activity of Civil Servants in Cyberspace*» describes the readiness of civil servants for professional activity in cyberspace and identifies factors that influence the professional activity of civil servants in cyberspace.

It has been established that the professional activity of civil servants in the digital environment is accompanied by both new opportunities for effective communication and an increase in social risks, primarily cyberbullying, cyberhate, procrastination, and digital fatigue.

The survey confirmed that a significant proportion of civil servants regularly use the internet not only for professional but also for personal purposes. At the same time, more than 40% of them admitted to being distracted daily by non-work-related online activities, and almost 22% constantly postpone work tasks in favour of secondary digital content. This indicates the spread of digital procrastination as a destructive factor that reduces productivity and complicates self-management for civil servants.

One of the most acute problems is the spread of cyberbullying – derogatory comments, insults and hostile actions on social networks, messengers, chats and even in private messages. Cyberbullying often concerns political topics, appearance, social status, gender, etc. Most respondents admit that these manifestations cause a strong emotional reaction: anger, sadness, anxiety, which complicates maintaining psychological stability during professional functioning.

It has been established that the threat is posed not only by experiencing cyber violence, but also by the participation of civil servants themselves in aggressive actions in cyberspace. A significant proportion of respondents admitted to spreading offensive content, which is an indicator of digital immaturity, low ethical resilience and the need for regulatory control of online behaviour.

A low level of institutional trust was also revealed: respondents are not ready to turn to management, the police or psychological services in the event of a cyber conflict, but instead rely mainly on informal sources of support – friends, family or no one at all. This indicates the need to create internal support mechanisms, increase trust in security services and develop psychological competence. Among the requests for support, educational (training, information resources), technical (blocking, security settings) and legal needs prevail. This indicates the importance of developing institutional programmes for digital awareness and professional training in the context of cybersecurity.

It has been proven that the professional activities of civil servants in cyberspace are determined by a combination of factors: individual psychological, social and communicative, and organisational and institutional. Taking these into account is critically important for the formation of a comprehensive system of digital adaptation and security for the civil service in the face of modern challenges.

The third chapter, Ways to Improve the Interaction of Civil Servants in Cyberspace, considers the possibility of implementing best international practices to improve the interaction of civil servants in cyberspace; directions and methods for developing the cyber psychological competence of civil servants; conducting preparatory measures to prevent cyberbullying and cyber hate in the Ukrainian civil service system.

The section presents an adapted model for implementing best international practices for civil servant interaction in cyberspace. It highlights successful approaches in the Netherlands, the United Kingdom, Canada, Bulgaria, India, and Estonia, as well as the experience of Singapore and Denmark, where ‘soft nudging’ mechanisms are implemented through subtle interventions in the form of self-prompts in digital and organisational spaces, the use of social norms as reinforcers of responsibility, and the use of sensory cues (colour, document structure) that increase the likelihood of a positive behavioural response. The effectiveness of such interventions is confirmed by the results of randomised controlled trials (RCTs),

which allow for the quantitative measurement of behavioural changes associated with the introduction of specific information formats or messages.

A logical continuation of the implementation of international experience was the development of cyberpsychological competence among civil servants as a key condition for increasing their digital behavioural maturity. Its structure (cognitive, emotional-regulatory, behavioural, ethical components) has been defined, and identified vulnerabilities (low stress resistance, tendency to reactive aggression, lack of skills to counter cyberbullying) have been analysed. A phased system for developing this competence through training modules, the work of HR psychologists, interactive simulations and monitoring of digital behaviour indicators has been proposed. A matrix of indicators for assessing the level of competence has been developed, combining quantitative and qualitative methods. The measurement of digital behavioural maturity is integrated into HR policy as a tool for ensuring a safe, ethical and psychologically stable digital environment.

The section also reveals the propaedeutics of cyberbullying and cyberhate as a component of digital security in personnel policy. The main forms of digital aggression and the reasons for its spread in the public sector are identified, and the risks to team performance (decreased trust, burnout, destruction of communication links) are analysed. It proposes scientifically based models of institutional response mechanisms, which include the creation of action protocols, responsible HR departments, digital ombudsmen, and the implementation of communication campaigns promoting zero tolerance for digital aggression using educational platforms, chatbots, and anonymous reporting forms.

Keywords: public administration, professional competence of public servants, e-government, civil service, human resource management in the civil service, cyberspace, cybersecurity.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Розділи в монографіях:

1. Кіберпсихологія у вимірах сучасного наукового дискурсу : монографія / авт. кол. : С. Хаджирадєва, Ю. Левін, М. Тодорова, М. Атанасов [та ін.]; за заг. ред. С. Хаджирадєвої. Одеса : Астропринт, 2024. 240 с. *(Особистий внесок : підготовлені підрозділи 1.5 «Професія «кіберпсихолог»: стан проблем та перспективи розвитку в Україні» та 4.1 «Критична життєва ситуація та особливості поведінки людини»).*

URL: https://www.astroprint.ua/uk/news/538

ISBN 978-617-8381-67-7

Статті, опубліковані у наукових фахових виданнях України:

2. Атанасов М. Аналіз світового досвіду у сфері удосконалення процесу взаємодії державних службовців у кіберпросторі. *Публічне управління та регіональний розвиток.* 2025. № 29. С. 1073–1101.

URL: https://pard.mk.ua/index.php/journal/article/view/547

DOI: 10.34132/pard2025.29.17

3. Атанасов М. В. Роль кіберхейту як складової частини кібербулінгу у системі розвитку персоналу на публічній службі. *Публічне управління та регіональний розвиток*. 2025. № 28. С. 606–627.

URL: https://pard.mk.ua/index.php/journal/article/view/494

DOI: https://doi.org/10.34132/pard2025.28.14

4. Атанасов М. В. Удосконалення компетентностей публічних службовців щодо управління місцевим розвитком на засадах процесного менеджменту. *Публічне управління та регіональний розвиток*. 2023. № 22. С. 937–963.

URL: https://pard.mk.ua/index.php/journal/article/view/389

DOI: 10.34132/pard2023.22.02

Інші опубліковані праці:

5. Атанасов М. В. Особливості сучасних методів оцінювання персоналу: переваги та недоліки. *Економіка та суспільство*. 2022. № 39

URL: https://economyandsociety.in.ua/index.php/journal/ article/view/1385

DOI: https://doi.org/10.32782/2524-0072/2022-39-38

6. Атанасов М. В. Оцінювання персоналу: сутність, види та алгоритм здійснення процедури оцінювання. *Економіка. Фінанси. Право*. 2022. № 6. С. 27–30.

URL: http://efp.in.ua/uk/journal-article/893

DOI: https://doi.org/10.37634/efp.2022.6.6

7. Ковтуненко К. В, Ковальчук О. В., Атанасов М. В. Персонал підприємства: сутність і підходи до визначення. *Економіка. Фінанси. Право*. 2021. № 9(1). С. 5–8.

(Особистий внесок : результати компаративного аналізу феномену «персонал підприємства)

URL: http://efp.in.ua/uk/journal-article/741

DOI: **:** https://doi.org/10.37634/efp.2021.9(1).2

Опубліковані праці у виданнях апробаційного характеру

8. Атанасов М. Вплив кіберхейту на процес управління персоналом: виклики та шляхи запобігання. *Ольвійський форум – 2025: стратегії країн Причорноморського регіону в геополітичному просторі.* Матеріали XXII міжнар. наук. конф. Чорноморського національного університету імені Петра Могили. Серія: Публічне управління та адміністрування: 16-22 червня. 2025 р., м. Миколаїв *:* Вид-во ЧНУ ім. Петра Могили, 2025. С. 134–137.

9. Лук'янчук О. М., Курилова Ю. П., Атанасов М. В. Особливості формування поняття «менеджмент персоналу». *Актуальні проблеми теорії та практики менеджменту.* Матеріали X Міжн. наук.-практ. конф. 28 травня 2021 р. : Державний університет «Одеська політехніка». Одеса: ДУ «Одеська політехніка», 2021. С. 85–86.

*(Особистий внесок : обґрунтовано базові підходи щодо визначення сутнісного значення поняття «менеджмент персоналу», а саме: функціональний, процесний та діяльнісний)***.**

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЄС – Європейський Союз.

КМУ – Кабінет Міністрів України.

НАДС – Національне агентство з питань державної служби України.

ОПВ – Органи публічної влади.

УЛР – Управління людськими ресурсами.

ШНМ – Штучні нейронні мережі.

ЗМІ – Засоби масової інформації

ВСТУП

Актуальність теми дослідження. Становлення інформаційного суспільства детерміновано інтенсивним розвитком інформаційно-комунікаційних систем, технологій, мереж, інформаційного та кібернетичного просторів, що зумовили посилення ролі соціальних мереж, їхній вплив на внутрішню і зовнішню суспільно-політичну ситуацію, стан додержання прав і свобод людини тощо.

Концепції публічного управління та адміністрування, зокрема New Public Management (NPM) – Нове державне управління; Good Governance – Належне урядування; E-Governance – Електронне урядування; Network Governance – Мережеве управління; Public Value Management – Управління публічною цінністю; Adaptive Governance – Адаптивне управління; Participatory Governance – Партисипативне управління та ін., вимагають нових підходів до вирішення проблем професіоналізації державних службовців, зокрема і вдосконалення системи управління персоналом на державній службі у вимірах взаємодії в кіберпросторі.

В сучасному науковому дискурсі концептуальний простір методологічних підходів розробки теорії управління персоналом представлений такими основними школами, концепціями, теоріями: класичні концепції – наукове управління; соціальна інженерія; комплексний підхід до організації праці і т. ін. (Ф. Тейлор, М. Емерсон, О. Гастев, П. Керженцев, М. Вітке та ін.); адміністративне управління (А.Файоль, М. Фоллет, Ч. Барнард та ін.); бюрократична організація (М. Вебер); концепція людських відносин (Е. Мейо, Ф. Ротлісбергер, Р. Лайкерт та ін.); концепція людських ресурсів і школа поведінкових наук (В. Скотт, У. Оучі, М. Фоллет, А. Маслоу, Д. Макгрегор та ін.); концепції ситуаційного підходу (Дж. Вудворт, В. Врум, М. Стівенсон, Ф. Фідлер, П. Герсі, К. Бланчард, Р. Блейк, Д. Моутон та ін.); концепції системного підходу: управління за цілями, концепція «7S» та ін. (І.

Ансофф, П. Дракер, Р. Лайкерт, Т. Пітерс, Р. Уотерман та ін.); концепції інституціонального підходу (Д. Норд та ін.); теорія людського капіталу (М. Беккер, Я. Мінсер, Т. Шульц та ін.); теорія стратегічного управління персоналом (М. Бір, П. Боксалл, Д. Гест, К. Легге, Д. Сторі, Д. Парселл, Д. Ульрих та ін.); компетентнісно орієнтований підхід (М. Армстронг, П. Сперроу, Дж. Хоткінсон, А. Фарнем) та ін.

Актуальність питання посилюється і тим, що Інтернет, представляючи нову систему соціальної взаємодії, інтегрує людей в єдину віртуальну спільність, в якій поступово виробляються свої норми і правила, засновані на особливостях і специфіці кіберпростору, що значно впливає на процеси соціалізації, особистісного, професійного та кар'єрного розвитку людини.

Ступінь розробленості теми дослідження. Аналіз вітчизняних та зарубіжних наукових фондів дозволяє констатувати, що, здебільшого, увага дослідників акцентувалася на таких проблемах як: реформування системи державного управління та державної служби в Україні (Н. Алюшина, В. Андріяш, Л. Антонова, М. Білинська, О. Васильєва, В. Ємельянов, В. Негода, Н. Олійник, А. Рачинський, С. Романюк, С. Серьогін, С. Сорока, О. Штирьов, А. Шульга та ін.); Е-урядування (Ю. Батир, В. Берч, Ю. Бисага, Я. Жовнірчик, Л. Івашова, В. Квасюк, І. Костенко, М. Міхровська, А. Помаза-Пономаренко, І. Лопатченко, О. Романчук, Г. Нечипорук, В. Чечерський та ін.); національна безпека (Р. Марутян, М. Орел, Г. Ситнік та ін.); методи та засоби забезпечення кібербезпеки в органах публічної влади (Ю. Білявська, В. Вишнівський, О. Довгань, І. Доронін, А. Пампуха, Я. Шестак та ін.); організаційно-правові засади діяльності публічних службовців в кіберпросторі (О. Антонова, Р. Татарінов, Ф. Федоренко та ін.); інформаційно-комунікаційна компетентність державних службовців (В. Волошин, Н. Драгомирецька, В. Дрешпак, В. Ніколаєв, А. Семенченко та ін.) тощо.

Недостатня теоретична розробленість означеної проблеми та недосконаліть практичних рекомендацій у цій сфері визначили вибір теми дисертаційного дослідження – «Управління персоналом на державній службі

у вимірах взаємодії в кіберпросторі».

Зв'язок роботи з науковими програмами, планами, темами. В основу дисертації покладено результати досліджень і розробок, отримані автором за безпосередньої участі в науково-дослідних роботах, що проводились в Чорноморському національному університеті імені Петра Могили з теми «Організація публічної влади в Україні, реалізація державної політики в соціогуманітарній сфері: культури, освіти, охорони здоров'я, інформаційної безпеки» (державний реєстраційний номер 0122U201631), де автором обґрунтувано рекомендації щодо підвищення ефективності управління персоналом на державній службі, а також представлено моделі інституційних механізмів реагування, що передбачають створення протоколів дій, відповідальних HR-підрозділів, цифрових омбудсменів, реалізацію комунікаційних кампаній нульової толерантності до цифрової агресії з використанням освітніх платформ, чат-ботів та анонімних форм повідомлення; та Державному університеті інтелектуальних технологій і зв'язку з теми «Крос-функціональний підхід щодо імплементації інструментарію кіберпсихології в концепцію когнітивного маркетингу» (ДР № 0124U004705), де автором було науково обґрунтовано теоретичні підходи, методи та моделі взаємодії в кіберпросторі, а також акцентовано увагу на роль кіберхейту як складової частини кібербулінгу в системі розвитку персоналу на публічній службі.

В якості експерта автор дисертації брав участь у проведенні досліджень та розробки практичних рекомендацій в міжнародних проєктах Німецької служби академічних обмінів, а саме: 1) «Навігація в цифровому просторі: стратегії підтримки молоді з урахуванням конфліктів» (DAAD-2024, ID-57709682), де автором обґрунтовано типові навігаційні маршрути в кіберпросторі, та чинники, що впливають на вибір молоддю цих маршрутів; 2) «Разом проти ненависті в Інтернеті: попередження та стратегії впливу на молодь в Німеччині, Киргизії, Молдові та Україні» (DAAD-2025, ID-57761453) – автором розроблено тренінгову програму для молодих публічних

службовців, журналістів та інших фахівців соціономічної сфери «Пропедевтика кіберхейту та кібербулінгу у сфері публічного управління та адміністрування».

Мета і завдання дослідження. *Метою* дослідження є науково-теоретичне обґрунтування та розроблення практичних рекомендацій щодо підвищення ефективності управління персоналом на державній службі у вимірах взаємодії в кіберпросторі. Для досягнення поставленої мети визначено такі *завдання*:

– виявити сутність феномену «кіберпростір» та з'ясувати особливості взаємодії в кіберпросторі з урахуванням ризиків віртуального середовища;

– встановити базові механізми взаємодії державних службовців у кіберпросторі, а також парадигмальні зсуви в управлінні персоналом на державній службі в умовах розвитку інформаційного суспільства;

– визначити, за результатами проведеного емпіричного дослідження, стан готовності державних службовців до професійної діяльності в кіберпросторі;

– встановити фактори, що впливають на професійну діяльність державних службовців у кіберпросторі;

– розробити та обґрунтувати рекомендації щодо підвищення ефективності управління персоналом на державній службі, а саме: можливостей імплементації кращих міжнародних практик з удосконалення взаємодії державних службовців у кіберпросторі; напрямів та методів розвитку кіберпсихологічної компетентності державних службовців; проведення пропедевтичних заходів щодо попередження кібербулінгу та кіберхейту в системі державної служби України.

Об'єкт дослідження – система управління персоналом на державній службі.

Предмет дослідження – управління персоналом на державній службі у вимірах взаємодії в кіберпросторі.

Методи дослідження. Для розв'язання завдань дослідження використано методи теоретичного рівня пізнання: аналіз і систематизація філософської, державно-управлінської, соціально-психологічної, навчально-методичної літератури з метою визначення стану і теоретичного обґрунтування проблеми дослідження; ідентифікації, екстраполяції – для виконання методологічної процедури перенесення інформації при опрацюванні літературних джерел й дослідженні еволюції проблеми управління персоналом на державній службі; класифікації – для подання предмета дослідження у вигляді множинності його елементів (таксонів); опитування – для визначення сучасних тенденцій управління персоналом на державній службі, а також базові проблеми, з якими стикається державні службовці в кіберпросторі; моделювання, структурно-функціональний та структурно-компонентний аналізи тощо.

Методи математичної статистики (статистична обробка результатів опитування та їх інтерпретація) з метою перевірки достовірності результатів дослідження. Розрахунки і обробка даних проводилися за допомогою комп'ютерних програм STATISTICA 8.0 та Microsoft Excel. Опрацювання отриманих результатів здійснено шляхом кількісного та якісного аналізу з використанням програмного забезпечення SPSS-21. Порівняння даних здійснено шляхом застосування критерію Манна-Уітні (U) та критерію Краскела-Уоліса (H). Дисертаційне дослідження здійснювалося на основі аналізу зарубіжних та вітчизняних наукових джерел, у тому числі інтернет-ресурсів.

Наукова новизна отриманих результатів визначається особистим внеском автора у вирішення актуального наукового завдання галузі знань «Публічне управління та адміністрування», яке полягає в теоретичному обґрунтуванні та розробленні практичних рекомендацій щодо підвищення ефективності управління персоналом на державній службі у вимірах взаємодії в кіберпросторі. Найбільш значущими результатами дослідження, що становлять наукову новизну, розкривають суть роботи та виносяться на

захист, є такі:

уперше:

– запропоновано науково обґрунтовані моделі інституційних механізмів реагування, що передбачають створення протоколів дій, відповідальних HR-підрозділів, цифрових омбудсменів, а також реалізацію комунікаційних кампаній нульової толерантності до цифрової агресії з використанням освітніх платформ, чат-ботів та анонімних форм повідомлення;

– визначено стан готовності сучасних державних службовців до професійної діяльності в кіберпросторі, а саме констатовано, що лише у 14,7% державних службовців високий рівень готовності до професійної діяльності в кіберпросторі; у 53,9% – мінімально достатній для виконання професійних обов'язків; у 31,4% – незадовільний, що вказує на поширення діджитал-прокрастинації як деструктивного чинника, що знижує продуктивність та ускладнює самоменеджмент державного службовця;

удосконалено:

– наукове уявлення про особливості управління персоналом державної служби, акцент зроблено на професійну взаємодію у кіберпросторі. Констатовано, що ризики в кіберпросторі охоплюють широкий спектр загроз як для організації (фінансові збитки, порушення конфіденційності даних, втрати репутації тощо), так і окремих осіб (порушення психічного здоров'я, професійне вигорання і т. ін.).

– організаційно-правовий, інформаційно-технічний, соціально-психологічний механізми професійного розвитку публічних службовців, за рахунок впровадження комплексних змін у систему державної служби України, зокрема: 1) обґрунтування концептуальних засад професійної діяльності державних службовців у кіберпросторі; 2) впровадження нової компетентнісної моделі професійної діяльності державних службовців у кіберпросторі; 3) модернізація технологій оцінювання готовності кандидатів на зайняття посад державної служби до здійснення професійної діяльності в

умовах цифрового урядування та розвитку інформаційного суспільства; 4) формування уявлень, цінностей і переконань про те, що цифрова компетентність, професійна мобільність, корпоративна та особиста кібербезпека стають стрижнем кар'єрного розвитку державних службовців;

набули подальшого розвитку:

– тезаурус галузі «Публічне управління та адміністрування», а саме: автором запропоновано під кіберпростором розуміти простір, обумовлений функціонуванням продуктів інформаційно-комунікаційних технологій, що дозволяють створювати складні системи взаємодій агентів (суб'єкти взаємодії) з метою отримання інформації, обміном та управління нею, а також здійснення комунікацій в умовах великої кількості мереж;

– методи підвищення ефективності управління персоналом у державній службі України, за рахунок обґрунтування адаптованої моделі імплементації кращих міжнародних практик щодо взаємодії державних службовців у кіберпросторі, де автором виокремлено успішні підходи Нідерландів, Великої Британії, Канади, Болгарії, Індії, Естонії, а також досвід Сінгапуру та Данії щодо застосування механізмів «м'якого підштовхування»;

– методи формування та розвитку професійної компетентності державних службовців, за рахунок формування кіберпсихологічної компетентності через навчальні модулі, роботу HR-психологів, інтерактивні симуляції та моніторинг показників цифрової поведінки. Розроблено матрицю індикаторів для оцінювання рівня компетентності, що поєднує кількісні та якісні методи;

– технології оцінювання кандидатів на зайняття посад державної служби, за рахунок вимірювання цифровоповедінкової зрілості особи. Доведено, що професійна активність державних службовців у цифровому середовищі супроводжується як новими можливостями для ефективної професійної комунікації, так і зростанням соціальних ризиків, насамперед – кіберзалякуванням, кіберхейтом, прокрастинацією та цифровою втомою;

– персонал-технології професійного розвитку державних службовців, за рахунок впровадження навчальних програм щодо пропедевтики кіберхейту та кібербулінгу в сфері публічного управління та адміністрування, що є запорукою забезпечення безпечного, етичного та психологічно стійкого цифрового середовища.

Особистий внесок здобувача. Дисертаційна робота є самостійною науковою працею автора. Основні ідеї та розробки, здійснені в рамках дисертаційної роботи, у тому числі ті, що характеризують наукову новизну, практичне значення дослідження, отримані автором особисто. У дисертації не використовуються ідеї та розробки співавторів, разом з якими опубліковано наукові праці. Так, у монографії «Кіберпсихологія у вимірах сучасного наукового дискурсу» (співавтори: С. Хаджирадєва, Ю. Левін, М. Тодорова та ін.) здобувачем були підготовлені підрозділи 1.5 «Професія «кіберпсихолог»: стан проблем та перспективи розвитку в Україні» та 4.1 «Критична життєва ситуація та особливості поведінки людини».

У науковій статті «Персонал підприємства: сутність і підходи до визначення» (співавтори: К. Ковтуненко, О. Ковальчук) здобувачу належать результати компаративного аналізу феномену «персонал підприємства».

В тезисах з теми «Особливості формування поняття «менеджмент персоналу» (співавтори: О. Лук'янчук, Ю. Курилова) – здобувачем обґрунтовано базові підходи щодо визначення сутнісного значення поняття «менеджмент персоналу», а саме: функціональний, процесний та діяльнісний.

Практичне значення отриманих результатів визначається тим, що основні теоретичні положення та висновки дисертації доведено до рівня конкретних пропозицій, що сприятимуть підвищення ефективності управління персоналом на державній службі у вимірах взаємодії в кіберпросторі. Можуть бути використані в науковій, законотворчій, управлінській, освітній, просвітницькій діяльності.

Основні теоретичні положення, запропоновані висновки та рекомендації використано:Державним університетом інтелектуальних технологій і зв'язку,

Чорноморським національним університетом імені Петра Могили, Комунальним закладом вищої освіти «Дніпровська академія неперервної освіти» Дніпропетровської обласної ради».

Апробація результатів дослідження. Науковий зміст основних положень і результатів дослідження та шляхи їх практичного застосування обговорювалися на 2 науково-практичних конференціях, зокрема: «Ольвійський форум – 2025: стратегії країн Причорноморського регіону в геополітичному просторі» (м. Миколаїв, 2025); «Актуальні проблеми теорії та практики менеджменту» (м. Одеса, 2021).

Публікації. Загальні положення дослідження висвітлено в 9 наукових публікаціях, з них: 1 - колективна монографія, 3 - статті у наукових фахових виданнях України (які входять до переліку МОН України); 3 – статті в інших виданнях; 2 - тези доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Повний обсяг роботи становить 254 сторінки, з них основного тексту – 200 сторінок. Дисертація містить 37 рисунків та 21 таблиць, 3 додатки. Список використаних джерел налічує 349 найменувань.

РОЗДІЛ 1
КОНЦЕПТУАЛЬНІ ЗАСАДИ УПРАВЛІННЯ ПЕРСОНАЛОМ НА ДЕРЖАВНІЙ СЛУЖБІ У ВИМІРАХ ВЗАЄМОДІЇ В КІБЕРПРОСТОРІ

Виходячи з того, що в науковому дискурсі концепція традиційно трактується як система поглядів, єдиний, визначальний задум або основна ідея, що лежить в основі певного розуміння явищ, процесів, або певної діяльності, пропонуємо розглянути обґрунтовану нами концептуальну модель управління персоналом на державній службі у вимірах взаємодії в кіберпросторі. Зауважимо, що дана модель концентрує дослідницьку увагу саме на предметній області феномену «управління персоналом на державній службі у вимірах взаємодії в кіберпросторі» через опис ключових термінів, понять визначень, а також теоретичних підходів, моделей, методів, інструментів і т. ін., що застосовується в описі цього процесу.

Для опису концептуальних засад управління персоналом на державній службі у вимірах взаємодії в кіберпросторі вважаємо доцільним викласти матеріал за такою логікою: 1) проаналізувати ґенезис феномену «кіберпростір» з акцентом уваги на термінологічному значенні понять «взаємодії» та «ризики віртуального середовища»; 2) описати базові механізми взаємодії державних службовців у кіберпросторі; 3) виявити парадигмальні зсуви в управління персоналом на державній службі в умовах розвитку інформаційного суспільства.

1.1. Ґенеза феномену «кіберпростір»: особливості взаємодії та ризики віртуального середовища

Дотримуючись наукових правил, перш за все, представимо тезаурус проблемного поля даного дослідження. На сьогодні в науковому дискурсі не існує усталеного трактування сутності поняття «кіберпростір». Більшість

вчених (І. Діордиця, В. Ліпкан, О. Ткаченко, В. Фурашев та ін.) зауважують на складності цього феномену, що обумовлює неоднозначність наукових підходів до його вивчення, зокрема наголошується на тому, що поняття «кіберпростір» доцільно трактувати ґрунтуючись на міждисциплінарних засадах [85; 198 та ін.].

Термін «кіберпростір» складається з двох елементів: «кібер», що означає «кібернетичний», та «простір». В даному контексті, «простір» є ключовим поняттям, тоді як «кібернетичний» вказує на специфічну орієнтацію чи природу цього простору. За енциклопедичним тлумаченням, слово «простір» може мати кілька значень, зокрема: протяжність, вмістилище, в якому розташовані предмети і відбуваються події [207]; поняття, що описує розмір, розташування та властивості об’єктів у світі [188]; набір елементів, що мають відносини, аналогічні звичним просторовим взаємозв’язкам, таким як близькість, дистанція тощо [13]; форма існування матеріальних об’єктів та процесів, підкреслюючи їх структурованість і вимірюваність, також характеризується такими атрибутами, як просторовість, єдність дискретності та безперервності [43] і т. ін.

В Законі України «Про основні засади забезпечення кібербезпеки України» кіберпростір визначається як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [146]. В документі ISO/IEC 27032 (Керівні принципи кібербезпеки) кіберпростір трактується як середовище існування, отримане у результаті взаємодії людей, програмного забезпечення і послуг в Інтернет за допомогою технологічних пристроїв і мереж, підключених до них, яке не існує у будь-якій фізичній формі [270].

На основі викладеного можна зробити попереднє припущення, що кіберпростір представляє собою середовище/систему, де матеріальні та

нематеріальні об’єкти і процеси існують разом з метою генерації, зберігання, трансформації та обміну інформацією. В певному сенсі, кіберпростір представляє собою віртуальну реальність, яка спирається на фізичну основу і має відчутні наслідки своєї активності та еволюції.

За висновками В. Богуш, В. Бровко, А. Войскунського, О. Мальцевої, М. Кастельє, В. Настрадін, М. Погорецький, В. Шеломенцев, О. Яницького та ін., кіберпростіру притаманні такі властивості як-от: просторова протяжність; сполучення дискретності та безперервності; взаємопроникнення матеріального та імматеріального; переплетіння абстракції та реальності; вплив на загальні реалії [94; 116; 119].

У дослідження В. Фурашева підкреслюється, що кіберпростір охоплює як фізичні аспекти, такі як обчислювальне обладнання, засоби комунікації, фізичні елементи телекомунікаційних мереж, розробку програмного забезпечення та інше, так і віртуальні компоненти, включаючи дані, обробку інформації, передачу даних тощо. Важливо підкреслити, що коли ми говоримо про фізичні компоненти у цьому контексті, ми маємо на увазі все те, що може бути сприйняте через зір, дотик чи інші чуття, відходячи від філософського розуміння матеріальності [197].

Осмислення терміну «кіберпростір», за словами Ю. Завгородньої, складається з різноманітних концепцій, серед яких вчена виділяє такі:

– простір, що виникає з взаємодій між людьми, програмним забезпеченням та інтернет-сервісами за допомогою цифрових пристроїв та мереж, який не має фізичного втілення;

– домен, де застосовуються цифрові технології для зберігання, зміни та обміну інформацією через мережеві системи та їх фізичну базу;

– сукупність мережевих та цифрових взаємодій, що охоплює контент та процеси його обробки;

– цифрова інфраструктура, що доступна через мережу Інтернет;

– комунікативне поле, створене мережею зв’язків між елементами кіберінфраструктури, включаючи цифрові обчислювальні системи, мережеві

з’єднання, програмне забезпечення та інформаційні бази даних [110; 119; 316 та ін.].

За думкою інших вчених (А. Бард, Н. Винер, У. Гибсон, Дж. Содерквіст, О. Холода та ін.), структура інформаційних агентів охоплює компоненти, як-от індикатор, тип, прототип, фільтр даних та динаміку людських дій і взаємодій з іншими програмами. Ці елементи спілкування стають ключовими у формуванні неперервного потоку кіберпростору. Людське існування занурене в реальний фізичний світ, проте існують також особистісний та психічний аспекти простору. Коли ми дивимося кіно, наші думки можуть бродити минулим чи уявляти майбутнє, або ж ми можемо втекти в світ фантазій і мрій, і саме в ці моменти наше існування розгортається у цьому психічному просторі [219]. Ми ж підтримуємо думку Д. Добринської, М. Токарева, О. Халік, А. Шамне, А. Шорнікова, Л. Юр’єва про те, що кіберпростір найчастійше характеризується як віртуальний простір, що складається з сукупності взаємодіючих користувачів, цифрових пристроїв та інформаційних систем, які використовують глобальні мережі для комунікації та здійснення різних видів діяльності [208; 13].

Окремо варто виділити групу дослідників, які розглядають кіберпростір як багатогранне соціальне, правове та технічне явище, що відзначається різноманіттям форм свого прояву та способів репрезентації сутності. На думку вчених (Н. Дженюк, В. Гордійчук, С. Євсеєв, О. Касілов, Б. Лазуренко, В. Ліпкан, О. Логінов, Ю. Саричев, О. Сєрков, П. Сніцаренко, Л. Харченко та ін.), кіберпростір доцільно розглядати як складову системи забезпечення національної, інформаційної та кібернетичної безпеки [176; 39; 86].

Зокрема, М. Погорецький та В. Шеломенцев визначають його як штучно створене електронне середовище, у якому в цифровій формі функціонують інформаційні об’єкти. Воно виникає завдяки роботі кібернетичних комп’ютерних систем управління й обробки даних, що надають користувачам можливість доступу до інформаційних та обчислювальних ресурсів, створення електронних продуктів, обміну повідомленнями, а також взаємодії у режимі

реального часу. Таке середовище забезпечує колективне використання ресурсів, у тому числі для надання інформаційних послуг чи ведення електронної комерції [119].

На переконання В. Бурячка, В. Толубка, С. Толюпи та В. Хорошка, кіберпростір варто розуміти як віртуальне комунікаційне середовище, сформоване системою зв'язків між користувачами й об'єктами інформаційної інфраструктури. До таких об'єктів належать електронні ресурси, мережі й системи різних форм власності, що працюють під управлінням автоматизованих систем. Вони використовуються не лише для обробки й передавання інформації задля задоволення потреб суспільства, але й можуть бути інструментом впливу на аналогічні об'єкти протилежної сторони [11].

Д. Дубов підкреслює, що кіберпростір є середовищем, сформованим сукупністю інформаційних процесів, які здійснюються в межах телекомунікаційних та інформаційних систем, об'єднаних спільними принципами і правилами, незалежно від їх форми власності [43].

На думку С. Рибки, Є. Кільчицького та О. Післегіна, кіберпростір являє собою організовану систему інформаційних процесів, пов'язаних зі створенням, зберіганням, передаванням та використанням інформації за участю людини. Особливу роль у цьому контексті відіграють об'єкти критичної інфраструктури держави, що функціонують на основі національної інформаційно-комунікаційної інфраструктури [162].

С. Гнатюк трактує кіберпростір як віртуальне середовище, що виникає внаслідок взаємодії користувачів із програмним і апаратним забезпеченням, мережевими технологіями (зокрема Інтернетом). Таке середовище слугує для підтримки й управління процесами обробки електронних інформаційних ресурсів з метою задоволення інформаційних потреб суспільства [25].

Таким чином, кіберпростір може розглядатися як локальне середовище, якщо використання комп'ютерної техніки відбувається без підключення до мережі, а також як розподілене середовище – у випадку з'єднання з локальною чи глобальною мережею передачі даних (зокрема Інтернетом). Слід

підкреслити, що основними характеристиками кіберпростору є: 1) його природа як інформаційного простору; 2) функція комунікативного середовища; 3) залежність від технічної (комп'ютерної) інфраструктури, що забезпечує його існування.

Зауважимо на особливостях взаємодії в кіберпросторі. Виходячи з того, що традиційно під взаємодією розуміється процес, коли декілька об'єктів або людей впливають один на одного, обмінюються інформацією, діями чи впливом, що змінює їхню поведінку або стан. Відомі психологи О. Саннікова та О. Чебикін зазначають, що це може бути у фізичному, соціальному, або будь-якому іншому контексті [168; 203]. Тоді як О. Михайловська, термін «взаємодія» трактує в більш широкому значенні «…будь-який вплив одного об'єкта на інший, що спричиняє зміни», що дозволило автору проаналізувати його сутнісні ознаки в системі «влада-громадськість». Вчена підкреслює, що взаємодія може бути прямою, коли об'єкти безпосередньо контактують, або опосередкованою, коли вплив відбувається через інші об'єкти або середовище [105]. Дотична з попередніми висловами є думка інших вчених (С. Гончар, О. Дибах, В. Мохор та ін.), які підкреслюють, що взаємодія – це двосторонній процес, де дії однієї сторони впливають на іншу, і навпаки, що призводить до зміни стану або поведінки цих сторін [109 та ін.].

В контексті вищенаведеного, на наш погляд, слід акцентувати увагу на таких ключових особливостях взаємодії в кіберпросторі як: кібербезпека, кіберзахист, кібергігієна, кіберпсихологічна готовність до взаємодії.

Кібербезпека, за висновками більшості вчених (Ю. Лісовська, В. Кононович, В. Копан, В. Корчинський та ін.) означає комплекс процесів, рекомендацій і технологічних рішень, які допомагають захистити від цифрових атак комп'ютерні системи, мережі, програми та дані від несанкціонованого доступу, зміни або знищення [5; 87 та ін.].

У середині 80-х років минулого століття були закладені основи стратегії інформаційної безпеки. Теорії виникали й розвивались у такій послідовності: 1) класична парадигма захисту інформації, заснована на контролі доступив; 2)

парадигма рубіжного захисту об’єктів інформаційної діяльності (принцип «кругової оборони»); 3) парадигма ешелонованої багаторівневої системи інформаційної безпеки інформаційних ресурсів і технологій; 4/5) мережецентрична парадигма інформаційної безпеки інформаційних ресурсів; 6) парадигма забезпечення кібербезпеки кіберсередовища підприємств, організацій та користувачів (в стадії розробки); реалізація «Стратегії кібербезпеки України». На черзі розробка соціально-центричної парадигми інформаційної безпеки особи, суспільства та держави, тобто національної безпеки.

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 [138]. Сьогодні кібербезпека є одним із пріоритетів у системі національної безпеки України, що підтверджується рядом нормативно-правових документів, що регламентують цю сферу, а саме: Закони України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про критичну інфраструктуру», «Про національну систему конфіденційного зв’язку», «Про національну безпеку України», «Про електронну ідентифікацію та електронні довірчі послуги», «Про кібербезпеку» та ін., а також затверджені Указом Президента України «Стратегія національної безпеки України», «Доктрина інформаційної безпеки України», «Національна стратегія розвитку інформаційного суспільства в Україні» та інші документи [136; 137; 140; 141;144;145 та ін.].

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.

Щодо кіберзахисту лише зауважимо на її основній меті – забезпечити конфіденційність, цілісність та доступність інформації, а також захистити від несанкціонованого доступу, зміни або втрати даних. Експерти з кіберзахисту (В. Вишнівський Є. Василіу, В. Кононович, В. Корчинський, С. Стайкуца, Р. Царьов та ін.) наголошують, що ефективність функціонування кіберпростору напряму залежить від наявності сучасної системи кіберзахисту [16] та концентрації ресурсів (інтелектуальні, технічні, фінансові та ін.) на її підтримку, утримання, розвиток, модернізацію тощо [197].

Важлива роль у процесі взаємодії в кіберпросторі вчені (В. Жогов І. Козубцов, В. Самелюк, Г. Форос та ін.) відводиться феномену «кібергігієна» яка включає в себе набір поведінкових правил, звичок і протоколів, які сприяють стабільному психосоматичному стану людини, а також знижують ризик кібератак [195]. Інші трактування терміну «кібергігієна» семантично повторюють змістовий контент один одного, що свідчить про одностайність поглядів у наці на цю проблему. Можна навести кілька прикладів: це, зокрема, заходи безпеки, спрямовані на захист користувацьких пристроїв від зараження шкідливим програмним забезпеченням і несанкціонованого отримання конфіденційних даних [207]; дотримання базових принципів цифрової (кібер) безпеки під час роботи в мережі Інтернет [162]; формування у користувача звички проактивного ставлення до питань кіберзахисту – як до елемента щоденної «цифрової гігієни», що дозволяє протидіяти кіберзагрозам та іншим викликам інформаційної безпеки [197] тощо

Кібергігієна та кібербезпека посідають ключове місце в умовах сучасного цифрового суспільства. Дотримання належних практик кібергігієни сприяє захисту персональних і корпоративних даних, а також мінімізує ризик поширення шкідливого програмного забезпечення та вірусів. Водночас ефективна система заходів кібербезпеки дозволяє запобігати кібератакам, підтримувати стабільність і працездатність інформаційних систем і мереж, а також зберігати репутацію користувачів та організацій. У контексті безперервного розвитку цифрових технологій надзвичайно важливо, щоб як

окремі особи, так і інституції приділяли першочергову увагу питанням кібергігієни й кіберзахисту, оскільки це забезпечує цілісність, безпечність та надійність цифрового середовища.

Для наукового аналізу цих явищ використовуються різні дослідницькі підходи. Один із них передбачає розгляд кібергігієни та кібербезпеки як складових більш широкої концепції кіберзахисту. Такий підхід дозволяє досліджувати їх у взаємозв'язку технологічних, процедурних і людських чинників. Інший напрям полягає у вивченні кібергігієни та кібербезпеки крізь призму соціально-психологічних аспектів, зокрема у контексті поведінки користувачів у мережі Інтернет.

При описі особливостей взаємодії в кіберпросторі не менша роль відводиться кіберпсихологічній готовності до взаємодії. За визначеннями, що подаються в інформаційно-довідковій літературі та словниках, «готовність» трактується як стан і властивість людини, яка може та бажає щось виконати [108]; згода зробити що-небудь [114]; стан або властивість людини, яка характеризується наявністю достатнього рівня знань, умінь, навичок, а також психологічної налаштованості для виконання певної діяльності або досягнення певної мети [70]; стан психічних функцій, що забезпечує високий результат при виконанні того чи іншого виду діяльності [98]

Аналіз наукових досліджень зарубіжних (Л. Кандибович, В. Лефтеров, О. Макаревич, І. Окуленко, В. Осьодло, Є. Потапчук, О. Хміляр, Ю. Широбоков та ін.) та українських вчених (Н. Білоконна, А. Коброслі, Л. Кондрашова, П. Лисак, М. Махній, З. Мірошник, О. Немеш, О. Самойленко та ін.) дозволяє констатувати що готовність характеризується як інтегральна якість, яка є результатом взаємодії двох таких характеристик – психоемоційний стан та психологічна характеристика особистості – які проявляються у взаємній збалансованості [71; 113; 167 та ін.]. За висновками В. Моляко, Л. Нерсесяна, А. Хавина та інших науковців, єдність афективного, емоційного початку, когнітивних утворень, переконань і поведінкових актів у вигляді навичок, стійких реакцій є виразом сформованості психологічної

готовності людини до певного виду діяльності [108; 114].

Розглядаючи кіберпсихологічну готовність до взаємодії ми підтримуємо думку вчених (А. Аттрілл-Сміт, К. Фуллвуд, М. Кіп, Д. Кусс, Т. Парсонс та ін.) про те, що це здатність людини адекватно сприймати, аналізувати та реагувати на інформаційні та психологічні загрози в кіберпросторі [216; 301]. Так, на погляд Ф. Інса, А. Гудімової, Н. Токаревої, А. Шамне, О. Халік та ін., це поняття охоплює як захист від зовнішніх впливів, так і внутрішню стійкість людини до негативних наслідків використання інформаційно-комунікаційних технологій [13; 34; 268 та ін.]

Важливо також акцентувати на ризиках віртуального середовища. Більшість вчених (В. Богуш, В. Бровко, Я. Мельник, Р. Мурасов, В. Настрадін та ін.) наголошують на тому, що ера інформації характеризується постійними кризами у всіх аспектах суспільного життя, що супроводжуються глобалізацією соціального і культурного контексту [110; 116 та ін.]. Це викликає ряд суспільних викликів, протиріч та конфліктів. Сучасне суспільство, обрамлене різноманітними теоретичними підходами (від «суперіндустріального» суспільства до «постлюдського») можна вважати епіцентром глибоких трансформацій та невідворотних ризиків.

За словами І. Федорової, концепція «ризику», яка проникла у соціальні, філософські та культурологічні дискурси, уособлює непередбачуваність і кризовий стан сучасного інформаційного суспільства. Вона асоціюється із загрозами, які створюються науковими технологіями та пов’язані з соціокультурними кризами, а також з ризиком техногенних катастроф, що загрожують глобальній цивілізації [194].

У науковому дискурсі відмічається, що ризики кіберпростору та інформаційного простору включають порушення конфіденційності, цілісності та доступності даних, а також атаки на інформаційні системи та мережі. До них належать фішинг, шкідливе програмне забезпечення, атаки на відмову в обслуговуванні, несанкціонований доступ та інші. Захист включає в себе використання надійних паролів, захист Wi-Fi мереж, та впровадження

комплексних систем захисту інформації [302; 303; 305 та ін.].

Відомі дослідники (А. Войскунський, В. Плєшаков, J. Suler, M. Whitty, Г. Young та ін.) наголошують, що численні соціальні зв'язки є важливими для підтримки функціонування соціальної мережі, однак для індивіда надмірна активність, що перевищує 150 контактів, може мати негативний вплив на психічний стан. Зокрема, це проявляється у зниженні самооцінки, виникненні депресивних симптомів, почутті самотності, загостренні конфліктних взаємин [18; 118; 275 та ін.].

Одним із поширених чинників психологічного дискомфорту є постійне порівняння власного життя з демонстрованим у соціальних мережах досвідом інших. Як відзначають H. Barton, O. Jordan, G. Kirwan, I. Connolly, V. Obidenkova, M. Palmer та ін., подібна практика веде до зниження почуття власної гідності [212; 275]. Саме з порівняння часто починається розвиток особистісних розладів, що посилюється нестійкістю життєвих цінностей та пошуком сенсу існування. Дослідження О. Воїнової, І. Кроса, В. Маркової, В. Плєшакова підтверджують, що низька самооцінка є фактором поглиблення депресивних станів [118 та ін.]. Водночас психологічна підтримка користувачів у кризових ситуаціях у віртуальному середовищі здатна запобігти розвитку тяжких форм депресії, які потребують медичного втручання.

У кіберпросторі міцні особисті взаємини є відносно рідкісним явищем, що зумовлює зростання соціальної ізоляції. Дослідження, проведене в Університеті Пердью (США, 2012 р.), свідчить: відторгнення або остракізм у віртуальних середовищах загрожує чотирьом базовим потребам людини – у приналежності, контролі, самооцінці та усвідомленні сенсу життя. Це, своєю чергою, негативно впливає на емоційну сферу, провокуючи афективні стани.

Повсякденна поведінка у віртуальних комунікаціях (спостереження, моніторинг тощо) відображає рівень довіри у відносинах. На думку C. Valeri, J. Weiss, A. Lau, K. McCarthy, у соціальних мережах поширеним явищем є токсичні стосунки, що супроводжуються болем і стражданнями однієї чи обох

сторін [279]. Вони часто ґрунтуються на повторюваній деструктивній поведінці партнера та здатні суттєво погіршувати психічне здоров'я. Особливо небезпечними є аб'юзивні взаємини, у яких агресор (аб'юзер) – через фізичне, сексуальне, психологічне або економічне насильство – порушує особисті кордони жертви, підпорядковуючи її волю. Як зазначають D. Dutton, P. Lenegan, R. Muelleman, R. Pakizer та ін., здебільшого аб'юзерами є чоловіки, хоча насильницька поведінка властива людям будь-якої статі [239; 336 та ін.].

Ще одним поширеним ризиком цифрового середовища є феномен FOMO (fear of missing out) – страх пропустити важливу подію. Це відчуття формується внаслідок постійного контролю за оновленнями у соціальних мережах і спричиняє тривожність, зниження самооцінки та відчуття соціального відчуження [113 та ін.].

Окрему увагу науковці (C. Morin, F. Mouton, A. Smith та ін.) приділяють проблемі депривації сну. Доведено, що регулярне користування соціальними мережами перед сном провокує безсоння та призводить до погіршення емоційного стану, зниження працездатності, появи тривожності й втоми [292; 322; 254].

Значний інтерес викликає й проблема адиктивної поведінки, що є різновидом девіантних форм активності. Вона пов'язана з неконтрольованим прагненням переживати надмірні емоції через зміну власного психічного стану, що з часом призводить до залежності [93; 156]. До цієї категорії належить і Інтернет-залежність. M. Griffiths запропонував операційні критерії для її діагностики: пріоритетність діяльності, зміна настрою, толерантність, симптоми відміни, конфлікти та рецидив.

У структурі нехімічних залежностей Інтернет-залежність може проявлятися у різних формах: нав'язливий «серфінг» (інформаційне перевантаження), надмірна комунікація в мережі, ігрова залежність, фінансові форми (азартні ігри, онлайн-покупки), кіноманія, а також кіберсексуальні відхилення. Такі розлади стають причиною поглибленої соціальної дезадаптації, а в ряді країн уже офіційно розглядаються як психічні хвороби,

що охоплюють до 15% населення, особливо молодь [321; 334; 335 та ін.].

Серед інших сучасних явищ виділяють: синдром фантомної вібрації – відчуття дзвінка чи повідомлення за його фактичної відсутності; номофобію – страх залишитися без мобільного телефону; кіберхондрію – тенденцію шукати медичну інформацію в мережі та перебільшувати симптоми захворювань [220; 335].

Окремим феноменом є так званий «ефект Google», що полягає у схильності забувати інформацію, яку легко відшукати за допомогою пошукових систем. Експерименти, проведені серед студентів Колумбійського та Гарвардського університетів, довели, що користувачі запам'ятовують не самі факти, а способи їхнього пошуку. Це створює ризики для когнітивних процесів і прийняття рішень у стресових та екстремальних ситуаціях, де відсутній доступ до Інтернету.

Узагальнюючи, можна стверджувати, що широкий спектр відхилень, синдромів і залежностей є прямим наслідком інтенсивної взаємодії людини з сучасними інформаційними технологіями.

Отже, в контексті даного дослідження під кіберпростором будимо розуміти простір функціонування продуктів інформаційно-комунікаційних технологій, що дозволяють створювати складні системи взаємодій агентів (суб'єкти взаємодії) з метою отримання інформації, обміном та управління нею, а також здійснення комунікацій в умовах великої кількості мереж. Кіберпростір характеризується у трьох вимірах: фізичному, інформаційному та соціальному. Особливості взаємодії в кіберпросторі обумовлені феноменами «кіберпсихологічна готовність», «кібербезпека», «кіберзахист», «кібергігієна». Ризики в кіберпросторі охоплюють широкий спектр загроз для організацій та окремих осіб, пов'язаних з операціями в цифровому середовищі. Ці ризики можуть призвести до фінансових збитків, порушення психічного здоров'я, конфіденційності даних, втрати репутації та інших негативних наслідків. Важливо розуміти ці ризики та вживати заходів для їх мінімізації.

1.2. Базові механізми взаємодії державних службовців у кіберпросторі

В контексті нашого дослідження під механізмом взаємодії будемо розуміти спосіб, яким різні частини системи впливають одна на одну для досягнення результату. У такому значенні кіберпростір є системою (множина взаємопов'язаних елементів, що утворюють єдине ціле), а її складові елементи взаємодіють із середовищем і між собою, і мають мету. Варто зауважити, що основною метою взаємодії державних службовців у кіберпросторі є забезпечення реалізації державної інформаційної політики, що передбачає вдосконалення захисту даних, комунікаційних та технологічних систем, а також підвищення обізнаності громадян про кібербезпеку. За висновками більшості вчених (О. Гончарук, М. Лесечко, Н. Савичук та ін.), державні службовці в кіберпросторі одночасно можуть мати статус як суб'єкта, так і об'єкта [28; 84]. Будучи в статусі суб'єкта системи кіберпростору державний службовець діє та/або здійснює впливи на її інші структурні елементи – тобто на об'єкти цієї системи. Однак, державний службовець може бути і об'єктом впливу інших суб'єктів, які знаходяться в системі кіберпростору, наприклад, коли йдеться про кібербулінг, кіберхейт тощо.

За результатами проведеного аналізу наукової літератури [7; 38; 65; 95; 201 та ін.] можна виділити три базових механізми взаємодії державних службовців у кіберпросторі, а саме: організаційно-правовий, інформаційно-технічний, соціально-психологічний. Розглянемо їх детальніше.

Організаційно-правовий механізм взаємодії державних службовців у кіберпросторі представляє собою систему взаємопов'язаних організаційних та правових засобів, що використовуються державними службовцями для досягнення цілей професійної діяльності. Вчені (Т. Гречко, С. Лісовський, О. Майданник, Н. Нижник, О. Остапенко, А. Романенко, С. Романюк, Л. Руденко, В. Сергієнко, О. Скакун, В. Федоренко та ін.) наполегливо доводять

важливість цього механізму в системі публічного управління та адміністрування [72; 91; 159; 174; 193 та ін.].

Щодо правових засобів інтегрованих в організаційно-правовий механізм взаємодії державних службовців у кіберпросторі, то їх регуляторна функція регламентована як міжнародними документами, так і діючими нормативно-правовими актами України (закони, укази Президента, постанови КМУ і т. ін.). Науковці (В. Берч, Ю. Бисага, А. Венглінська, Г. Лук'янова, Г. Нечипорук, Ю. Размєтаєва, О. Романчук, В. Чечерський та ін.) зазначають, що більшість нормативно-правових актів України відповідають міжнародним стандартам та вимогам в цій сфері [89; 161; 165 та ін.].

Акцентуємо на документах, які найбільш важливі для регулювання взаємодії державних службовців у кіберпросторі, зокрема:

– *Закони України:* «Про інформацію» [140], «Про доступ до публічної інформації» [129], «Про основні засади забезпечення кібербезпеки України» [146], «Про державну таємницю» [127], «Про звернення громадян» [139] та ін. Важливо акцентувати, що в Законі України «Про інформацію» державна інформаційна політика визначається як сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації;

– *Укази Президента України:* «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади» [128]; «Про Доктрину інформаційної безпеки України» (затверджено рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року) [148; 149] та ін.;

– *Постанови та розпорядження КМУ:* «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади» [147], «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» [153], «Про роботу центральних і місцевих органів виконавчої влади щодо забезпечення відкритості у своїй діяльності, зв'язків з громадськістю та взаємодії з засобами масової інформації» [150], «Про затвердження Порядку

сприяння проведенню громадської експертизи діяльності органів виконавчої влади» [137], «Про затвердження Регламенту Кабінету Міністрів України» [135] і т. ін.

Одним з основних елементів організаційно-правового забезпечення функціонування кіберпростору є Закон України «Про основні засади забезпечення кібербезпеки України» [146]. Цей законопроєкт встановлює юридичні рамки та структурні основи для забезпечення захисту фундаментальних прав людей, спільнот, а також національної безпеки в кібернетичному просторі. Він окреслює ключові мету, стратегії та основоположні принципи, якими керуватиметься українська державна політика в області кіберзахисту. Також визначаються права та обов'язки органів влади, комерційних та некомерційних організацій, а також окремих осіб і громадян у цій сфері. Закон трактує кібербезпеку як «захищеність життєвоважливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [146].

Більшість дослідників (В. Берч, А. Кубко, О. Романчук, В. Федоренко та ін.) описуючи проблеми кібербезпеки, зауважують, що особи, які порушують законодавчі норми в областях національної безпеки, цифрового зв'язку та інформаційного захисту, де кіберпростір служить ареною або засобом вчинення протиправних дій, підлягають відповідальності згідно із законом, як передбачено цивільним, адміністративним чи кримінальним законодавством [81; 165; 193].

В контексті аналізу правових засобів, інтегрованих в організаційно-правовий механізм взаємодії державних службовців у кіберпросторі, важливо підкреслити діяльність органів публічної влади щодо налагодження міжнародних відносини у сфері кібербезпеки. Україна, відповідно до міжнародних угод, погоджених з іншими країнами, співпрацює у сфері

кібербезпеки з зарубіжними державами, їхніми правоохоронними та спеціальними службами, а також з міжнародними установами, задіяними у протидії міжнародним кіберзагрозам. Україна, враховуючи необхідність забезпечення безпеки індивідів, суспільства та держави, на своїй території приймає заходи проти осіб, залучених до кібернетичних злочинів або терористичних актів у кіберпросторі, включно з тими випадками, коли такі злочини були сплановані або здійснені за межами України, але мали негативний вплив на країну, а також у інших ситуаціях, передбачених міжнародними договорами, ратифікованими Верховною Радою України.

Ще одним законом, який є дотичним до кіберпростору є Закон України «Про медіа» [143]. Дотичним він є через те, що багато суб'єктів кіберпростору задіяні у створенні або цитуванні медіаконтенту та відповідних творів. За висновками правників (О. Хорватова, Ю. Пухір та ін.), цей закон має на меті гарантувати здійснення права на вільне висловлення думок, доступ до широкого спектру точної та актуальної інформації, підтримку розмаїття поглядів та вільний обмін інформацією, охорону державних інтересів України та прав споживачів медіа [200; 201]. На думку В. Мільо, Д. Проценко, М. Рожило, О. Теребус та ін., регулювання медійної сфери на основі принципів прозорості, об'єктивності та непристрастності, сприяння здоровій конкуренції, рівності та незалежності медійних організацій і встановлює юридичний статус, процедуру створення, функціонування та компетенцію Національної ради України з питань телебачення та радіомовлення [63; 106; 155; 164].

У межах наукової дискусії, яку ведуть дослідники (Ю. Бажал, О. Баранов, Ю. Бисага, М. Демкова, С. Дзюба, О. Ємельяненко, І. Жиляєв, О. Кілієвич, І. Клименко, Д. Ковальчук, І. Коліушко, А. Кундій, К. Линьов, О. Мертенс, Г. Нечипорук, І. Розпутенко, О. Романчук, А. Семенченко, О. Соловйова, В. Чечерський, С. Чукут та ін.) щодо формування та результативності державної інформаційної політики, увага зосереджується на низці ключових аспектів. Серед них: забезпечення громадянам вільного

доступу до інформації; розбудова національних інформаційних систем і мереж; укріплення матеріально-технічних, фінансових, організаційних, правових і наукових засад інформаційної діяльності; підвищення ефективності використання інформаційних ресурсів; стимулювання їх постійного оновлення, збагачення та збереження; створення комплексної системи інформаційної безпеки; активізація міжнародного співробітництва у сфері інформації та гарантування інформаційного суверенітету України [37; 45; 52; 53; 74; 161; 165; 178; 205 та ін.].

Також відзначимо проблемне поле наукового дискурсу щодо організаційних засобів, інтегрованих в організаційно-правовий механізм взаємодії державних службовців у кіберпросторі. Сьогодні дискусійними залишаються питання щодо реформування органів публічної влади, а також їх ефективного функціонування в умовах сучасних глобальних викликів, зокрема тих, що пов'язані з розвитком інформаційного суспільства та кіберпростору.

Створення в Україні цифрових державних структур підкріплюється ключовим стратегічним документом європейських країн, який керує процесом цифровізації – Цифрова стратегія для Європи (Digital Agenda). Вчені (К. Богатирьов, Н. Гришина, А. Гриценко, Ф. Інс, І. Іртищева, І. Крамаренко, О. Купчишина, В. Ракіпов, А. Шевченко та ін.) наголошують, що цифрове управління неминуче стає передовою практикою [29; 61; 280; 320 та ін.].

В Україні було вирішено створити спеціалізований орган влади, що носитиме відповідальність за процеси цифровізації в адміністративному секторі. Рішенням уряду від 18 вересня 2019 року, згідно з розпорядженням № 856, було встановлено регламент діяльності Міністерства цифрової трансформації. Цей орган призначений відігравати ключову роль у державному апарату, сприяючи розробці та впровадженню національної політики у сферах, що охоплюють цифровізацію, розвиток цифрових сервісів та інфраструктур, електронне урядування, електронну демократію, поширення інформаційних технологій, впровадження електронного документообігу,

підвищення рівня цифрової грамотності та захисту цифрових прав громадян, розвиток відкритих даних, та багато іншого.

Додатково, були вжиті заходи для створення відповідних підрозділів у структурі міністерств і виконавчих органів на регіональному рівні, зосереджених на питаннях цифрового розвитку та цифрової трансформації, що дозволяє забезпечити ефективну координацію та впровадження відповідних ініціатив у всій країні. У контексті центральних виконавчих органів передбачено введення посад заступників, які б відповідали за напрямки цифрової трансформації, з метою оптимізації процесів та підвищення ефективності управління цифровими проектами на державному рівні.

Основними цілями Міністерства цифрової трансформації на 2024 рік заявлені: переведення 100 % усіх публічних послуг для громадян та бізнесу онлайн; забезпечення 95 % транспортної інфраструктури, населених пунктів та їхні соціальні об'єкти доступом до високошвидкісного інтернету; навчання 6 млн українців цифрових навичок; підвищення частки IT у ВВП країни до 10 % [6; 7; 16].

Ініціатива Міністерства цифрової трансформації України «Держава у смартфоні» є втіленням цього технологічного стрибка, пропонуючи користувачам зручний доступ до державних послуг через електронний підпис у мобільному додатку або на ноутбуці. На погляд експертів (А. Алюшина, О. Карпенко, А. Семенченко та ін.) проєкт «Цифрова держава» є ключовим елементом в розвитку електронного уряду, який має на меті зробити доступними онлайн усі послуги, що надаються державними установами [8; 9; 23 та ін.]. Величезний обсяг інформації про громадян збирається і систематизується, деякі дані залишаються відкритими для загального доступу, інші – захищені і доступні лише за наявності спеціальних прав. Захищеність цієї системи відповідає вищим стандартам безпеки, забезпечуючи надійний захист персональних даних.

Участь України в світовій інформаційній спільноті передбачає втілення чотирьох основних рівнів електронних послуг, що включають інформаційне

забезпечення, комунікацію, транзакції та участь в управлінні державою. Досягнення в реалізації цих послуг, за висновками В. Волошина, Д. Ковальчука, А. Кундія, В. Ніколаєва, І. Хребрія та ін., дуже помітні: громадяни можуть реєструвати бізнес онлайн, подавати заявки на соціальні виплати, отримувати довідки та інші послуги без потреби відвідувати державні установи [170; 178 та ін.]. Вчені також вказують на те, що втілення концепції «Цифрової держави» зустрічає певні виклики, зокрема, обмежене покриття інтернетом і низький рівень цифрової грамотності серед населення [165; 169]. Проте, розробники ініціативи активно працюють над подоланням цих бар'єрів, впроваджуючи освітні програми та адаптуючи послуги для всіх категорій користувачів. За висновками Р. Емран, розвиток «Цифрової держави» в Україні відкриває нові можливості для громадян, спрощуючи взаємодію з державними структурами і роблячи цей процес більш зручним і прозорим [49].

Таким чином, можна констатувати, що організаційно-правовий механізм взаємодії державних службовців у кіберпросторі представляє собою систему взаємопов'язаних організаційних та правових засобів, що використовуються в публічній сфері для досягнення цілей держави у сфері суспільних відносин. До організаційних засобів відносимо комплекс заходів, спрямованих на структурування та управління професійною діяльністю державних службовців, процесами, ресурсами та інформацією в органах державної влади для досягнення поставлених цілей та забезпечення їх ефективного функціонування. Правові засоби, будучи елементами правової дійсності, виступають в якості регуляторів взаємодії державних службовців у кіберпросторі, обумовленого нормами міжнародного та національного права, галузевими нормативно-правовими актами тощо.

Аналізуючи інформаційно-технічний механізм взаємодії державних службовців у кіберпросторі варто звернути увагу на концептуальні основи мережевого зв'язку, що були сформульовані Дж. Ліклідером у 1960 р. та удосконалюються його послідовниками (H. Duiin, St. Littgart, R. Biddulph, S. Balashek A. Libenlnan, K. Stevens, S. Kasowski, C. Forgic та ін.) до сьогодні [257;

259; 261 та ін.]. Ідею ж Інтернету розробив П. Беран, який видав серію з 12 томів, в яких виклав ідею створення децентралізованої мережі, заснованої на передачі даних у вигляді окремих блоків. Така мережа, на його думку, могла б вистояти в умовах потенційного ядерного конфлікту. Д. Девіс, працівник Національної Фізичної Лабораторії у Великобританії, у 1965 році винайшов концепцію пакетної комутації та запропонував створення національної мережі для комерційного обміну даними [337].

Перша машина мережі ARPANET була розгорнута 1-го вересня 1969 року в університеті Каліфорнії, розташованому в Лос-Анджелесі. Обладнана комп'ютером «Honeywell 516», ця система мала в своєму розпорядженні 12 кілобайтів RAM (оперативної пам'яті) [337]. Поширення Інтернету є результатом науково-технічного прогресу, який разом із біотехнологічними досягненнями (здатність людства маніпулювати генетичною інформацією, контролюючи біологічну еволюцію) має глибокий вплив на глобальну спільноту. На погляд О. Данильяна та О. Дзьобань, нова ера інформатизації суспільства характеризується можливістю отримання деталізованих даних, що відтворюють реальність, формуючи комплексне уявлення про об'єкт [35].

Упродовж останніх років темпи зростання кількості інтернет-користувачів сповільнилися до 4 %, що може вважатися логічним наслідком оскільки більшість населення Землі (6 з 10 осіб) вже має доступ до мережі. Водночас, згідно з останніми даними, 2,9 мільярда людей (37% світового населення) все ще залишаються поза Інтернетом, причому значна частина з них проживає у Південно-Східній Азії [198].

У ранні 1990-ті роки була розроблена система Gopher для відшукання та обміну інформацією. Ця платформа пропонувала структурований перелік посилань на документи, цифрові ресурси та інші переліки, дозволяючи їм зв'язуватися між собою через Інтернет для доступу до контенту з різних джерел. Gopher знайшов широке застосування в академічних кругах, де він допомагав ділитися інформацією по всьому кампусу, а також у великих

корпораціях, які потребували ефективних систем для організації та управління даними.

В той час, у Європейській організації з ядерних досліджень (CERN) в Швейцарії вже була розроблена альтернатива. Тім Бернерс-Лі працював над системою управління інформацією, яка дозволяла інтегрувати гіперпосилання в текст, уможливлюючи перехід між документами. Він розробив сервер для публікації таких документів та браузер для їх перегляду, який отримав назву «WorldWideWeb» або «www» («Всесвітня павутина»). Початкова версія програми була представлена у 1991 році, але дві ключові події 1993 року кардинально змінили ситуацію на користь нової системи.

13 квітня 1993 року CERN оголосив код WorldWideWeb вільним для використання та модифікації, що відкрило шлях до його масового розповсюдження та подальшої еволюції без будь-яких ліцензійних обмежень.

Концепт «Всесвітньої мережі» зародився в уяві Тіма Бернерса-Лі, який у 1989 році Бернерс-Лі розробив мову розмітки гіпертексту, HTML, яка стала фундаментом для створення веб-документів. Ця мова забезпечила доступ до інформації в Інтернеті для будь-якого користувача з будь-якого місця світу. Робота над HTML велася в CERN, що згодом отримав статус колиски Інтернету через свій вклад у розвиток веб-технологій. Розробка універсального протоколу обміну даними став основою для створення децентралізованої інформаційної системи, відкритої для кожного. Це був протокол HTTP для передачі гіпертекстових документів.

Таким чином, у 1990 році відбулося запуск першого проєкту Всесвітньої мережі, що поклало початок новій ері обміну інформацією [180]. Наявність і постійне введення в експлуатацію нових інтернет-сервісів безперервно посилює вплив мережі на різні сфери повсякденного життя людей, включаючи і державне управління. Використання Інтернету в комерційних цілях, яке спочатку було обмежене, в останні часи демонструє стабільне зростання. Дедалі більше організацій вдаються до Інтернету для здійснення реклами, маркетингу, надання послуг, укладення угод, проведення платежів,

комунікації внутрішньої та міжнародної, проведення ринкових аналізів, планування стратегій розвитку, обміну фаховою інформацією, керування персоналом і вербування нових співробітників.

Розширення масштабів Інтернету та пов'язаних з ним технологій, які впливають на зростання обсягів споживання, виробництва та обміну інформацією, спонукає до переходу на цифрові платформи. Це, в свою чергу, вимагає введення правового регулювання вказаної сфери [67].

За висновками вчених (А. Кирилюк, Л. Піддубна та ін.) сьогодні активність різноманітних інтернет-сервісів та постійна поява нових посилюють вплив цифрового простору на всі аспекти життя сучасної людини. Численні компанії організації застосовують інтернет для маркетингових цілей, реклами, надання послуг, укладання угод, проведення фінансових операцій, забезпечення комунікації, проведення ринкових досліджень, планування стратегічного розвитку, обміну спеціалізованою інформацією, управління кадрами та набору нових співробітників [67]. Вчені також стверджують, що еволюція інтернету та супутніх йому технологій сприяє збільшенню частки цифрового споживання, виробництва та обміну даними, що стимулює перехід на цифрові платформи та вимагає правового регулювання у цій сфері [4; 288; та ін.].

Говорячи про цифрові технології та їх вплив на формування кіберпростору зауважимо на тому, що у стратегічному плануванні Європейського Союзу, зокрема у стратегії «Європа 2020», технології інформації та комунікацій (ІКТ) відіграють центральну роль. «Цифрова адженда для Європи», яка є однією з семи ключових ініціатив цієї стратегії, служить основою для розвитку подібних стратегічних документів в країнах, що входять до Організації економічного співробітництва та розвитку (ОЕСР).

Програма «Горизонт 2020» (2014–2020 рр.), яка була ключовою ініціативою Європейського Союзу в цей період, спрямована на підтримку досліджень та інновацій, відповідає основним цілям стратегії «Європа-2020» через фокусування на трьох основних напрямках: 1) розвиток передових

наукових досліджень; 2) посилення промислового лідерства; 3) вирішення глобальних соціальних проблем, зокрема через застосування ІКТ.

Українські ІТ-експерти (О. Борняков, О. Вискуб, М. Федоров, О. Шелест та ін.) та лідери в сфери публічного управління та адміністрування (А. Ахламов, В. Дрешпак, О. Карпенко, Ю. Пігарєв, А. Семенченко та ін.) неодноразово підкреслювали, що програма «Горизонт 2020» сприяло розвитку ІКТ в Україні завдяки міжнародній співпраці та інтеграційним процесам [169; 170; 171 та ін.].

В міжнародному експертному середовищі останні десятиріччя підкреслюється плив ІКТ на економічне зростання та ринок праці. Дослідження, проведені компанією Booz&Company та глобальною консультаційною фірмою Pricewaterhouse Coopers, вказують на те, що цифровізація сприяла зростанню світового виробництва на 200 млрд доларів у 2022 році, а також додала 6 млн робочих місць [217; 329 та ін.].

Додаткові дані, зібрані у співпраці з університетом Чалмерса та компанією Ericsson на основі аналізу 33 країн ОЕСР, показали, що подвоєння швидкості широкосмугового інтернету може сприяти зростанню ВВП на 0,3% [44, с.120-121]. Вчені також акцентується на необхідності для країн з перехідною економікою, таких як Україна, приділяти особливу увагу процесам цифрової трансформації. Це дозволить підвищити рівень технологічної оснащеності та інфраструктури, забезпечити фінансування масштабних інженерних ініціатив і пом’якшити існуючий розрив у глобальних рейтингах порівняно з більш розвинутими країнами світу.

У світлі сучасних викликів в Україні, за ствердженнями голови Національного агентства з питань державної служби Н. Алюшиної, розвиток цифрових компетенцій серед управлінського персоналу стає все більш актуальним. На думку вченої, це включає в себе навички роботи з інформаційними ресурсами, вміння організовувати інформаційний обмін, конструювання та прогнозування робочих цілей за допомогою ІКТ, підтримку електронної демократії та протидію інформаційному виключенню [159 та ін.].

У дослідженнях Г. Лопушняк та Р. Миляник рекомендується у сфері державної служби сприяти підвищенню рівня знань у сфері ІКТ та програмних продуктів, збільшення використання Інтернету для збору та аналізу даних, а також стимулювання постійного самовдосконалення та освоєння нових методів роботи з цифровими технологіями [88].

Цифрові технології вплітаються у повсякденне життя кожної людини та впливають на його скорішу інтеграцію до кіберпростору. Саме поява нових поколінь гаджетів, допоміжних систем, тощо безпосередньо прискорює цей процес. Нові смартфони, розумні системи в автомобілях, бездротовий інтернет, технології 5G, оптоволоконний інтернет за PON технологіями роблять взаємодію усій суб'єктів економіки, побуту тощо та інших інституцій скорішою за принципом «тут і зараз».

Отже, сучасні цифрові технології (бездротовий інтернет, технології 5G, оптоволоконний інтернет за PON технологіями і т. ін.) формують сьогоднішній кіберпростір у якості альтернативного виміру, де люди проводять до половини свого життя, відвідуючи маркетплейси замість магазинів, інформаційні канали у месенджерах замість покупки газет, дивлячись фільми та серіали на сайтах замість відвідування кінотеатрів і т. п.

Окремо слід акцентувати на феномені «штучний інтелект. Видатний дослідник Г. Лі зазначив, що незважаючи на критичну необхідність чіткого визначення ШІ для ефективного регулювання та управління, досягнення консенсусу серед експертів і філософів щодо цього питання залишається недосяжним. Це частково пояснюється відсутністю узгодженого розуміння базової концепції «інтелекту» на філософському рівні, як це було підкреслено на зустрічі провідних мислителів у 2014 році, де брали участь Д. Деннет, П. Черчланд, Д. Чалмерс та інші видатні вчені.

Першу спробу сформулювати термінологічне значення поняття «штучний інтелект» зробив Дж. Маккарті на Дартмутській конференції у 1956 році, визначивши його як науку і технологію створення інтелектуальних машин і програм [267]. Оксфордський словник надає більш детальне

визначення, включаючи розуміння людського інтелекту, як теорію і розробку комп'ютерних систем, здатних виконувати завдання, які традиційно вимагають людського інтелекту, включаючи візуальне сприйняття, розпізнавання мови, прийняття рішень і переклад між мовами.

Пізніше Шейн Легг і Маркус Хаттер пропонують оцінку ШІ як здатності системи досягати цілей у широкому спектрі умов. Сучасне розуміння штучного інтелекту виходить за рамки традиційних визначень, описуючи його як розробку адаптивних агентів, здатних пристосовуватися до нових, невідомих ситуацій на основі досвіду і досягати цілей, які були б недосяжними для звичайних комп'ютерних систем [4].

Штучний інтелект представляє собою наукову концепцію, що займається створенням апаратних або програмних систем, які імітують види діяльності, що традиційно вважаються за прояви людського інтелекту. Штучний інтелект знаходить застосування в широкому спектрі від шахових програм до самостійних роботизованих агентів, впливаючи на різні аспекти суспільного життя. До інтелектуальних завдань входять: розпізнавання зразків, аналіз ситуацій, логічне міркування, асиміляція нових даних, процеси навчання та самоосвіти, а також розробка стратегій для досягнення конкретних цілей.

Інтелектуальна система може функціонувати під зовнішнім керівництвом, але властивою їй є здатність самостійно управляти своїми діями. Система націлена на певну мету і прагне до її досягнення через оптимальне планування дій. Система аналізує навколишнє середовище та коригує свою поведінку відповідно до змін, оцінюючи їх як позитивні чи негативні.

Особливістю інтелектуальних систем є їхня здатність до оновлення первинних знань, що вважається однією з основних характеристик. Ця властивість, відома як здатність до навчання, включає як зовнішнє навчання, так і процес самоосвіти.

В результаті, інтелектуальну систему можна визначити як автономну кібернетичну систему, що володіє комплексом знань про оточення і здатна на основі прямого сприйняття та аналізу ситуації розробляти стратегії дій для досягнення своїх цілей, а також до самовдосконалення та навчання [160].

Однією з особливостей є також те, що штучний інтелект характеризується відсутністю компонента, який забезпечує самостійну відповідальність за прийняття кінцевого вибору, тобто елементу, що надає системі здатності «усвідомлювати відповідальність за ухвалені рішення» [55].

Прогрес у вивченні структури людського мозку дозволив дослідникам зрозуміти, що мозок складається зі ста мільярдів нейронів, кожен з яких взаємопов'язаний з тисячами інших нейронів. Це відкриття стало основою для створення математичних моделей нейронних мереж, відомих як штучні нейронні мережі (ШНМ).

Наукова спільнота зосередилася на вивченні потенціалу штучних нейронних мереж для застосування у системах, що вимагають прийняття рішень. Однією з ключових передумов для ефективності нейромереж є їх здатність адаптуватися та навчатися, що призвело до пошуку методів навчання для ШНМ. Важливий внесок у цю область зробив Д. Хебб у 1949 році, запропонувавши метод, який демонструє здатність штучних нейронних мереж до навчання, що поклало основу для розвитку численних алгоритмів тренування ШНМ.

ШНМ базуються на математичних моделях, що дозволяють системі генерувати відповіді на вхідні сигнали або дані. Результатом діяльності такої системи є числовий вивід, який потім інтерпретується людиною.

З подальшим розвитком ШНМ, які представляють собою взаємодію великої кількості простих математичних моделей нейронів, здатних виконувати перетворення вхідних даних у вихідні, дослідження у цій області починають переплітатися з когнітивними науками, розширюючи горизонти застосування і розуміння ШНМ [17].

Варто також зазначити правові аспекти взаємодії із штучним інтелектом. Сприйняття штучного інтелекту та робототехніки як учасників цивільного права вважається недоречним і може призвести до юридичної невизначеності. Використання поняття «електронна особа» у законодавчих документах є непродуманим на даному етапі, оскільки це не надає чіткого розуміння щодо їхнього правового статусу, цивільної відповідальності, захисту прав споживачів, та захисту персональних даних. Крім того, наділення їх статусом суб'єктів передбачає застосування до них норм про захист їх прав, що передбачає наявність у них власного вибору та можливості самостійно керувати своєю поведінкою згідно з принципом диспозитивності, а також володіння правами та обов'язками на рівні з іншими учасниками правових відносин. Логічніше було б розглядати роботів та штучний інтелект як об'єкти цивільних прав. Регулювання питань цивільно-правової відповідальності у контексті споживчих відносин дає підстави вважати штучний інтелект продуктом. Впровадження технологій штучного інтелекту у таких галузях як медицина чи державне управління вимагає розглядати їх як об'єкти з підвищеною небезпекою, що може сприяти ефективнішому захисту прав користувачів. Враховуючи технологічний прогрес та цифровізацію, особлива увага має бути зосереджена на ролі людини в інтеракціях, пов'язаних з новітніми технологіями [92].

Таким чином, можна стверджувати, що інформаційно-технічний механізм взаємодії державних службовців у кіберпросторі представляє собою сукупність технічних засобів, програмного забезпечення та процедур, які забезпечують обмін інформацією та взаємодію між різними системами, пристроями або користувачами. Цей механізм включає в себе як апаратну частину (комп'ютери, мережеве обладнання тощо), так і програмну (операційні системи, програми обміну даними, протоколи зв'язку).

Соціально-психологічний механізм взаємодії державних службовців у кіберпросторі представляє собою систему взаємопов'язаних конструктів (Я-концепція, когнітивні функції, емоційний інтелект, цінності, мотивація,

групова динаміка і т. ін.), а також сукупність процесів, за допомогою яких державні службовці впливають один на одного, формують спільні уявлення, емоції та поведінку в процесі спілкування та спільної діяльності в кіберпросторі. Відомі вчені (Л. Анрі, Д. Майерс, С. Максименко, Ю. Машбіц, Т. Ньюкомб, М. Смульсок, Дж. Твенге, О. Чебикін та ін.) при розгляді соціально-психологічного механізму взаємодії здебільшого акцентують увагу на таких аспектах, як соціальна перцепція, соціальна фасилітація, групові норми, лідерство та інші [175; 293; 294; 328 та ін.].

Дослідники J.Watson, M. Whitty та ін., відмічають, що взаємодію в кіберпросторі слід аналізувати як процес обміну інформацією, ідеями, та досвідом між користувачами, що використовують комп'ютерні мережі, цифрові пристрої тощо [316; 334; 335 та ін.]. Соціально-психологічна складова кіберпростору приваблює увагу дослідників у галузі психології. За словами багатьох авторів (G. Kelly, D. Myers, N. Robinson та ін.), саме кіберпростір, охоплюючи взаємодію людини з технологією, стає мовною репрезентацією психологічної реальності особистості, відображаючи їх думки, емоції, страхи, інтереси та життєві історії [275; 293; 310 та ін.].

Інтернет привносить елементи постмодерної культури в повсякденне життя молоді, надаючи доступ до чужих культурних форм і створюючи нові культурні арени. За висновками вчених (А. Лучинкина, Н. Сенченко, С. Шевченко та ін.) інтернет-культура виявляється більш фрагментованою, різноманітною та інтерактивною порівняно з традиційними ЗМІ. Сучасна молодь, як перше покоління кібергенерації, зростає у світі, де мас-медіа та комп'ютерні технології формують їхню культурну ідентичність [90; 321].

Дж. Сулер у своєму дослідженні «Психологія кіберпростору» акцентує на унікальних психологічних характеристиках кіберпростору, які впливають на поведінку особистості. Однією з ключових особливостей є зниження відчуттів через обмеження сенсорного досвіду у віртуальному середовищі, хоча сучасні технології все більше намагаються залучити наші відчуття, створюючи ілюзію присутності. Текстуальність, як переважання текстової

взаємодії в Інтернеті, відіграє значну роль у самовираженні та міжособистісних відносинах, дозволяючи індивідам представити свою ідентичність та сприймати інших в онлайн-просторі. Таким чином, кіберпростір стає ключовим елементом у формуванні особистісної ідентичності та соціальних взаємин сучасної молоді [58].

В контексті взаємодії із державними службовцями в кіберпросторі важливу роль також грають стереотипи, що формуються за допомогою інтернет спільноти по відношенню до інститутів влади та її елементів. У сучасному інформаційному просторі соціальні стереотипи набувають форму через широкий спектр інтернет-матеріалів: від візуальних зображень до текстових повідомлень. Інтернет стає полем для поширення таких стереотипних виразів, як популярні цитати, типові коментарі, сатиричні зображення, інтернет-жарти та інші подібні явища. Для глибокого аналізу соціальних стереотипів критично важливо вивчати їх прояви в інтернеті, розуміючи унікальність кіберпростору з його правилами та поведінковими моделями, які впливають на створення та поширення соціальних стереотипів.

Соціальні стереотипи в інтернет-комунікаціях мають свої особливості, такі як швидке розповсюдження і зникнення, а також можливість використання різних форм виразу одночасно. Водночас, багато їх характеристик схожі на стереотипи, які існують у позамережевому світі.

Критичне ставлення до соціальних стереотипів як до причини соціальних конфліктів не є цілком виправданим, оскільки проблема не в самому понятті стереотипу, а в людській природі та сприйнятті. Зміна окремих стереотипів не змінить людську суть, але може трансформувати реальність. Повне позбавлення від стереотипів неможливе, але можливе їх усвідомлення та контроль над ними для протидії маніпуляціям свідомістю. Соціальні стереотипи існують у динаміці між старим та новим: знищення одного стереотипу призводить до формування іншого.

На погляд В. Роєнко, вивчення соціальних стереотипів вимагає аналізу їхніх проявів у повсякденному житті та в інтернеті, де вони можуть бути

представлені у формі установок, соціальних норм, шаблонного мислення та інших форм впливу. Інтернет стає резервуаром соціальних стереотипів, які можуть існувати виключно в цифровому просторі, лише у реальному світі, або в обох контекстах [163].

У монографії «Кіберпсихологія: у вимірах сучасного наукового дискурсу» розкрито вплив нейронних мереж на особистість. На думку дослідників (Ю. Левін, М. Тодорова, С. Хаджирадєва, Н. Шиліна та ін.), такий вплив зумовлений низкою чинників. По-перше, розвитком нейротехнологій, адже сучасне суспільство переживає інтенсивний прогрес у сфері інформаційних технологій, включно зі штучним інтелектом та нейромережами. По-друге, важливим є соціокультурний контекст, що набуває дедалі більшого значення для суспільної безпеки та добробуту. По-третє, актуальною є потреба у психологічному аналізі, оскільки вивчення особистості та самосвідомості традиційно займає центральне місце у психологічних дослідженнях [69].

Сучасні наукові розвідки підтверджують, що на особистість впливають як зовнішні фактори, так і внутрішні процеси, зокрема функціонування мозку та нейронних систем. Розширення можливостей нейромереж ставить перед наукою низку питань щодо їхнього впливу на психіку, зокрема на розвиток самосвідомості, емоційної сфери, мотивації та формування особистісних характеристик.

Узагальнюючи, можна виокремити низку теоретичних підходів, які дозволяють пояснити ці процеси у вимірах кіберпростору та застосувати їх для аналізу управління персоналом у державній службі. Серед них: теорія особистісних конструктів Дж. Келлі, теорія рис Р. Кеттелла, психологічна концепція особистості Г. Айзенка, теорія соціального пізнання А. Бандури, психоаналітична теорія З. Фрейда, гуманістична психологія, біхевіоризм, когнітивна психологія та ін. (див. табл. 1 у Додатку А).

Сучасні психологічні теорії у цифрову епоху справляють відчутний вплив на розвиток технологій та різних сфер людської діяльності. Їхнє

практичне застосування простежується у сфері проєктування інтерфейсів, створенні психологічних тестів, програмах розвитку особистості, що сприяє формуванню більш ефективних та орієнтованих на людину технологічних рішень. Відповідно, опора на такі теоретичні засади може стати основою для вироблення практичних рекомендацій щодо вдосконалення системи управління персоналом на державній службі в умовах становлення інформаційного суспільства.

Окремої уваги заслуговують як теоретичні, так і прикладні аспекти функціонування нейронних мереж. Вони відтворюють роботу нервової системи людини та тварин, складаючись із численних штучних нейронів, об'єднаних у шари, які обробляють дані за принципами, подібними до функціонування біологічних нейронних структур. На думку більшості науковців (L. Jeffrey, S. Hochreiter, J. Schmidhuber та ін.), поєднання системного використання нейротехнологій із принципами функціонування нейронних мереж та їхньою здатністю до навчання відкриває нові перспективи. Це дає змогу створювати точніші моделі роботи мозку, а також розробляти інноваційні методики когнітивної стимуляції й терапії психічних розладів [266; 271; 314 та ін.].

На базі нейронних мереж уже реалізовано широкий спектр застосувань і технологій, орієнтованих на підвищення когнітивних здібностей людини. Такі здобутки становлять потенційну основу для їхнього практичного використання у професійному розвитку державних службовців. Узагальнені результати подано в табл. 2 у Додатку А.

На думку фахівців (D. Rumelhart, G. Hinton, R. Williams, R. Sutton, A. Barto, J. Watson, M. Whitty, L. Wilbur, M. Higley, J. Hatfield, Z. Surprenant, E. Taliaferro, D. Smith, A. Paolo та ін.), нейронні мережі суттєво впливають на когнітивні процеси людини, що відкриває нові перспективи для сучасної науки. Основні сфери їх застосування охоплюють такі аспекти як-от: обробку та аналіз великих обсягів інформації, що покращує навчальні та аналітичні здібності людини; пам'ять і запам'ятовування; розпізнавання образів (зокрема,

згорткові нейронні мережі, натхненні роботою зорової кори мозку, дозволяють підвищувати ефективність обробки візуальної інформації); мовні навички (нейромережі сприяють моделюванню та аналізу мовних структур і патернів); а також процеси прийняття рішень, допомагаючи удосконалювати аналітичні здібності та вибір оптимальних рішень [334; 335; 336 та ін.].

Важливим аспектом є те, що ефективне інтегрування нейромереж у різні сфери діяльності людини, зокрема професійну, потребує врахування низки психологічних факторів. До них належать: приватність та конфіденційність даних; довіра користувачів до технологій; прозорість і зрозумілість рішень, які приймаються нейромережею; визначення відповідальності за результати прийнятих рішень; а також вплив на емоційно-мотиваційну сферу, зокрема можливі реакції користувачів – від тривожності через автоматизацію процесів до позитивного творчого підйому та мотивації.

У цьому контексті особливе значення має психологічна підтримка користувачів для зменшення стресу та тривожності, пов’язаної з використанням технологій. Врахування зазначених психологічних аспектів дозволяє розробляти ефективні стратегії впровадження нейромереж, мінімізувати потенційні негативні наслідки та максимізувати позитивний ефект у різних галузях діяльності. Таким чином, можна стверджувати, що складовими соціально-психологічного механізму взаємодії державних службовців у кіберпросторі є соціальна перцепція, групові норми, цінності, переконання і т. ін., які впливають на особисту, групову та професійну поведінку державних службовців у кіберпросторі.

Отже, базовими механізмами взаємодії державних службовців у кіберпросторі є: організаційно-правовий, інформаційно-технічний, соціально-психологічний. Саме через призму розуміння функціонування цих механізмів можна оцінювати ефективність взаємодії державних службовців у кіберпросторі, а також удосконалювати/модернізувати таку взаємодію, під впливом зовнішніх та внутрішніх факторів.

1.3. Парадигмальні зсуви в управління персоналом на державній службі в умовах розвитку інформаційного суспільства

Відомі вчені (В. Голубь, С. Телешун, Ю. Сабадаш, А. Сундук, І. Петрова С. Ситник, І. Рейтерович, О. Пухкал та ін.) зазначають факт того, що людство стоїть на порозі радикальних перетворень у житті цивілізації, пов'язуючи це із змінами в геополітиці [57; 127; 158; 184 та ін.], соціально-економічних відносинах [187 та ін.], культурних традицій [185 та ін.]. Однак найбільш небезпечними вважаються зміни в технології мислення людини, впровадженням штучного інтелекту і т. ін. [69].

У зазначеному контексті можна констатувати, що існуюча парадигма управління персоналом на державній службі знаходиться в процесі парадигмального зсуву. Це означає, що основоположна модель, система понять, уявлень, методів, цінностей і переконань управління персоналом на державній службі знаходяться під впливом значних змін та трансформаційних перетворень, які приймаються певною спільнотою (науковою, культурною, соціальною) та визначають новий спосіб мислення, вирішення проблем.

В науковій літературі ґенеза таких парадигмальних трансформацій описана в термінах моделей державної служби, основні з них такі: меритократична модель державної служби, модель класичної бюрократії, модель нової публічної служби (New Public Service), постмодерністська модель публічної служби (Post-NPS (NPS – New public Service)), партнерська модель публічної служби [190; 192 та ін.]. Зауважимо на трьох основних передумовах, що генерують появу парадигмальних зсувів в управлінні персоналом на державній службі в Україні, зокрема: 1) цифровізація державного сектору; 2) корпоративна та особиста кібербезпека державних службовців; 3) взаємодія масмедіа та державної влади. Деталізуємо їх.

Так, в епоху формування суспільства, заснованого на інформації, структура державного регулювання мусить адаптуватися до принципів е-управління. Впровадження цифрових ініціатив у сфері управління вимагає

оновлення традиційної системи державного регулювання, щоб відповідати сучасним викликам. На погляд Н. Драгомарецької, В. Дрешпака та ін., з одного боку, необхідно реформувати діяльність урядових інституцій, аби їх робота була більш відкритою для громадськості, конкурентною та орієнтованою на потреби громадян [41]. Це передбачає переосмислення ролі держави в умовах публічного адміністрування, розширення участі громадськості та передачу певних управлінських повноважень місцевим спільнотам. З іншого боку, держава має зберегти свої основні функції у сфері захисту прав громадян, забезпечення дотримання законодавства та регуляторного контролю [41].

В сучасних умовах система державного регулювання набуває більшої адаптивності, формуючи нові відносини між урядом, суспільством та сектором бізнесу. Ключовим елементом в цій взаємодії стає цифрова комунікація, включаючи обмін електронними документами та використання електронного підпису для зв'язку між різними рівнями уряду (G2G), а також забезпечення зв'язку між урядом, громадянами (G2C) та бізнесом (G2B). Таким чином, через систему державного управління враховуються виклики, що постають перед інформаційним суспільством, і реалізуються ключові державні функції у сфері організації, координації, регулювання та контролю.

С. Коулмен вказує на потребу розширення традиційної моделі трьохсторонньої комунікації в демократії до п’ятисторонньої, що включає: зв’язок від Уряду до Громадянина (G2C); зв’язок від Громадянина до Уряду (C2G); зв’язок від Представника Уряду до Громадянина (R2C); зв’язок від Громадянина до Представника Уряду (C2R); комунікація між Громадянами (C2C).

Так, функціональність сервісу «урядова взаємодія G2G» можна описати як оптимізацію витрат уряду, прискорення процесу обігу документів у його структурах, збільшення ефективності контролю над діями окремих установ та їх співробітників, стимуляцію конкуренції та професійного розвитку серед співробітників, а головне – запобігання корупційним проявам.

Розглядаючи можливості та функції цифрового урядування як сучасної моделі управління, необхідно виділити його вплив не тільки на взаємовідносини між громадянами та владою, але і на внутрішню структуру самого уряду – між його відділами, рівнями, підрозділами. В результаті змінюється не тільки цифрова інфраструктура виконавчої влади, але і в цілому структура державного управління. На погляд А. Семенченка та В. Дрешпака, саме тому поняття «електронний уряд» більш точно буде висловлено як цифрова держава, цифровий апарат влади, цифрова інфраструктура держави, держава інформаційної епохи [46].

В контексті впровадження цифрового взаємодіяти G2G, ключовим є перехід до цифровізації всіх управлінських процесів на всіх рівнях державної влади, до цифровізації міжвідомчого взаємодія, створення комп'ютеризованих систем для підтримки усіх функцій взаємодії цих структур з населенням та бізнес-структурами. Більшість вчених (Т. Забейворота, А. Каммані, Р. Сафина, Д. Спасібов, З. Фанг та ін.) вважають, що цифрове урядування передбачає не тільки використання ІКТ та створення цифрових ресурсів, але й розробку відповідного правового поля. Наприклад, необхідно законодавчо визначити, що електронний документ є первинним документом, з яким можна працювати в цифровому форматі. Це передбачає прийняття законів про цифровий підпис, про електронний документообіг, про захист даних, про освіту і сертифікацію співробітників, про форми співпраці державних структур з IT-компаніями тощо [57; 180; 250].

Цифрове урядування, а зокрема модуль G2G, передбачає оптимізацію використання ресурсів, контроль та забезпечення прозорості обігу документів в його структурах, підвищення контролю над діяльністю різних відомств та службових осіб, стимулювання конкуренції та кваліфікації серед працівників, та найважливіше – запобігання корупції.

Розглядаючи можливості та функції електронного уряду як новітньої моделі державного керування, особливу увагу слід звернути на внутрішню реорганізацію урядових структур. Електронний уряд вносить зміни не тільки

в зв’язки між громадянами та владою, але й у внутрішню динаміку уряду, включаючи взаємодії між різними гілками, рівнями та підрозділами. Зміни торкаються не лише цифрової інфраструктури, а й загальної системи державного управління. Таким чином, поняття «електронний уряд» можна розширити до «електронної держави» або «електронної державної адміністрації».

А. Семенченко зазначає, що впровадження G2G-сектору передбачає цифровізацію усіх аспектів державного управління на всіх рівнях, включаючи міжвідомчу кооперацію та створення систем, здатних підтримувати всі функції взаємодії з населенням та бізнес-структурами [169; 170]. Таким чином, електронний уряд вимагає не лише технологічних інновацій, а й розробки відповідних законодавчих актів. Важливо законодавчо визначити, що електронний документ є первинним і може використовуватися в електронному вигляді. Це також включає необхідність регулювання електронного підпису, електронного документообігу, захисту даних, а також стандартів навчання та сертифікації для держслужбовців.

Важливою є також співпраця уряду з IT-компаніями, що вимагає чіткого законодавчого регулювання для запобігання перенесенню існуючих проблем у сферу електронного урядування. Не можна ігнорувати і факт того, що перехід на електронний уряд пов’язаний з великими витратами на інфраструктуру, програмне забезпечення, навчання персоналу та інше. За О. Андреєвою контроль, який забезпечує G2G, допомагає запобігати неефективному використанню ресурсів та іншим зловживанням. Врешті, G2G сприяє оптимізації ресурсів уряду, підвищує ефективність міжурядової взаємодії та допомагає підвищити кваліфікацію та компетентність держслужбовців, сприяючи їхньому професійному росту та розвитку [3].

У дослідженнях А. Барікової, С. Оксентюк доводиться, що використання електронного уряду на рівні G2B/B2G сприятиме зниженню витрат для держорганів за рахунок впровадження технологій аутсорсингу та створенню прозорої системи державних закупівель (eProcurement). Централізована

система електронних закупівель передбачає створення онлайн-платформи, де урядові установи будуть публікувати тендерну документацію та умови проведення торгів, що підвищить конкурентність і забезпечить справедливий вибір постачальників [5; 115].

Бізнес-структури, що витрачають чимало часу на звітність перед контрольними органами, отримають можливість автоматизувати процеси: оплата соціальних внесків за співробітників; подання ПДВ-декларацій та отримання інформації про перевірки; реєстрація нових підприємств; звітність до статистичних органів; митне декларування.

Наразі інформування громадян здійснюється переважно через ЗМІ та не має системного характеру, обмежуючи доступ до необхідних документів. Електронний уряд відкриє для громадян такі можливості:

- зменшення часу на отримання державних послуг та їх надання;
- доступ до онлайн-форм, запису на прийом, отримання ліцензій та дозволів, подання податкових декларацій, заявок на соціальну допомогу, реєстрацію персональних документів та інше;
- використання комплексних послуг завдяки інтеграції державних органів, уникнення необхідності подання паперових довідок;
- легкий доступ до законів, правил, державної політики та послуг, а також до проектів законів, звітів та бюджетних документів;
- можливість активної участі в управлінні державою та контролі за діяльністю уряду через концепцію електронної демократії;
- залучення громадян, що проживають за кордоном, до життя країни через онлайнові платформи та електронні петиції, а також спрощення процесу голосування через Інтернет [66; 169].

У сучасному суспільстві виникає все більша потреба в ефективній системі надання соціальних послуг громадянам на локальному рівні. Це включає розробку інтегрованої системи інформаційних технологій та відповідного законодавчого забезпечення, а також пошук ефективних державних механізмів для забезпечення прав громадян, включаючи надання

якісних соціальних послуг. Не менш важливою є підготовка спеціалістів у соціальній сфері до роботи з різними категоріями клієнтів, зокрема через впровадження інформаційних технологій.

В Україні застосування новітніх інформаційних технологій у сфері соціальних служб є предметом обмеженого числа досліджень. Фахівці підкреслюють значення онлайн-інструментів для профілактики соціальних проблем як ефективний інструмент, особливо враховуючи специфіку аудиторії інтернету, до якої переважно належить молодь.

Популярними онлайн-інструментами для заохочення користувачів до здорового способу життя та запобігання соціальним проблемам є веб-сайти та соціальні платформи, такі як соціальні мережі, блоги та відеохостинги. Електронні розсилки також використовуються, хоча рідше. Серед переваг використання онлайн-технологій в соціальній роботі виділяють економічну ефективність, здатність одночасно охоплювати велику аудиторію, швидке поширення інформації та можливість підтримки двостороннього зв'язку з цільовою аудиторією.

Проте, використання онлайн-технологій має і свої обмеження, включаючи потребу в значних зусиллях для підтримки активності онлайн-ресурсів, обмеження в зміні поведінки через однієї лише інформації та труднощі у взаємодії з різними аудиторіями через один ресурс.

Консультування онлайн пропонує доступність, відкриває нові можливості для залучення клієнтів та забезпечує комфорт і анонімність. Однак, воно також передбачає необхідність постійної онлайн-присутності, може ускладнити перехід клієнта до особистих консультацій та вимагає зусиль для відстеження реакцій клієнтів.

Впровадження онлайн-технологій змінює стандартну практику соціальної роботи, сприяючи розвитку нових форм взаємодії. Це створює не тільки технологічні, а й етичні виклики, а також вимагає адаптації навчальних програм для підготовки майбутніх соціальних працівників.

Вивчаючи тему розвитку цифрових навичок у контексті державного управління, ми досліджуємо концепцію «цифрової компетентності». Аналіз літератури виявляє різноманіття інтерпретацій цього терміну. Це розмаїття у розумінні обумовлене персональними науковими поглядами авторів і контекстом їхніх досліджень. Ключові концептуальні підходи до визначення «цифрової компетентності» розкриваються через призму різних наукових дискусій та методологічних рамок [96].

Цифрова грамотність означає здатність ефективно, обачливо та етично користуватися цифровими інструментами у процесі освіти, в професійному середовищі та при взаємодії в соціальному контексті [54; 78].

Рамка цифрової компетентності громадян України включає наступні ключові компоненти:

основи комп'ютерної грамотності – володіння комп'ютерними та мобільними пристроями, базовим програмним забезпеченням, прикладними застосунками, використанням Інтернету та онлайн-сервісів, а також управління цифровою ідентичністю;

інформаційна грамотність та робота з даними – уміння здійснювати пошук, перегляд та фільтрацію даних і цифрового контенту; критично оцінювати та інтерпретувати інформацію; управляти даними та реалізовувати власні інформаційні запити; забезпечувати самореалізацію у цифровому суспільстві;

створення цифрового контенту – розробка, редагування та інтеграція цифрового контенту; дотримання авторського права та ліцензій; базові навички програмування; творче використання цифрових технологій;

комунікації та взаємодія у цифровому середовищі – комунікація та обмін даними через цифрові технології; співпраця в онлайн-середовищі; цифрове громадянство, використання е-послуг та електронного підпису; дотримання правових та етичних норм, мережевого етикету;

безпека в цифровому середовищі – захист пристроїв та безпечне підключення до мережі; захист персональних даних та приватності;

забезпечення безпеки в Інтернеті; охорона прав споживачів від шахрайства та зловживань; турбота про здоров'я та благополуччя; захист навколишнього середовища;

розв'язання проблем у цифровому середовищі – вирішення технічних проблем; визначення потреб та їх технологічне задоволення; самооцінка рівня цифрової компетентності та усунення прогалин; застосування цифрових технологій для вирішення життєвих задач; навчання протягом життя, професійний та особистісний розвиток у цифровому середовищі [96; 204].

Отже, з цифровізацією державного сектору з'являються нові виклики для системи управлінні персоналом на державній службі, а саме: осучаснення інфраструктури та дизайну робочих місць державних службовців; розширення переліку ІТ-компетентностей; налагодження/удосконалення механізмів взаємодії державних службовців у кіберпросторі тощо.

Ми підтримуємо точку зору вчених (В. Кононович, В. Євдокимов, С. Савчук та ін.), які кібербезпеку визначають як комплекс процесів, рекомендацій і технологічних рішень, які допомагають захистити важливі системи, дані й мережу від цифрових атак [166; 182]. У зазначеному контексті важливо відмітити організаційно-рольову функцію державних службовців, вони будучи частиною системи державної служби України відчувають на собі небезпеку в кіберпросторі. На погляд експертів з кібербезпеки ефективна програма з кібербезпеки включає фахівців, процеси й технологічні рішення, які зменшують ризик перерв у роботі органів державної влади, крадіжки даних, репутаційної шкоди внаслідок атак тощо.

На погляд більшості вчених (В. Бурячок, Н. Дженюк, Д. Дубов, С. Євсеєв, О. Касілов, Б. Лазуренко, В. Ліпкан, О. Логінов, О. Сєрков, Л. Харченко та ін.), державним службовцям слід враховувати такі основні види кіберзагроз: атаки «відмова в обслуговуванні» (DoS) і розподілені атаки на відмову в обслуговуванні (DDoS); атаки з використання фішингу та соціотехнік; внутрішні загрози; загрози для ідентичності; зловмисні програми з вимогою викупу; порушення безпеки корпоративної електронної пошти;

удосконалені постійні загрози (АТР); шкідливе програмне забезпечення (віруси, зловмисні програми з вимогою викупу, шпигунські програми, хробаки) та ін. [11; 39; 42; 85 та ін.].

Вчені (Р. Андерсон, М. Бишоп, Д. Пинкус, М. Ранум, Г. Морисетт, П. Нойман, М. Ховард, Б. Чесвік та ін.) у своїх дослідженнях багато уваги приділяють слабкій безпеці (candy security) [267 та ін.]. Аналіз причин порушень інформаційної безпеки в органах державної влади дозволяє виділити п’ять основних факторів:

1) безвідповідальність державного службовця – свідомі або випадкові дії, спрямовані на компрометацію інформації, що можуть бути пов’язані з умисним шкодою;

2) зондування системи – ситуації, коли службовці для самоствердження або експерименту взаємодіють із системою безпеки, порушуючи її правила, навіть якщо наміри є нешкідливими;

3) корисливі інтереси – цілеспрямовані дії щодо подолання системи захисту для доступу до конфіденційної інформації, що зберігається та обробляється в органах влади;

4) переманювання фахівців – стратегія, спрямована на ослаблення конкурента та отримання додаткової інформації;

5) психологічний вплив специфіки діяльності — державні службовці, які працюють із конфіденційною інформацією, піддаються стресу та ризику психологічних зривів через обмеження свободи, потребу зберігати таємницю та постійне відчуття загрози втрати секретних документів.

Людський фактор є ключовим джерелом вразливості інформаційної безпеки. За висновками експертів (Д. Грицишен, В. Євдокимов, С. Савчук , С. Корзун), ефективне забезпечення безпеки в органах влади базується на системному підході, що поєднує технологічну інноваційність, інженерну точність та соціально-психологічне моделювання поведінки людей [30; 75]. Володіння цими інструментами дозволяє формувати поведінкові моделі, за яких особи «добровільно» й «самостійно» діють у визначеному соціальному

напрямку.

У науковому дискурсі феномен «людський фактор» (англ. Human factor) визначається як сукупність соціальних якостей особистості: ціннісних орієнтирів, моральних принципів, норм поведінки, життєвих планів, рівня знань, професійних і соціальних навичок, а також уявлень про соціально значущі елементи життя [69]. Згідно з С. Васьківською, людський фактор є потенційним і актуальним джерелом інформаційних проблем при використанні сучасних технологій [14].

Інформаційно-психологічна безпека особи у вузькому розумінні – це стан захищеності психіки від негативного впливу деструктивної інформації, яка може призводити до спотвореного сприйняття реальності [69]. У широкому розумінні вона включає: а) належний рівень підготовки особистості для забезпечення захисту життєвих інтересів та гармонійного розвитку; б) здатність держави створювати умови для гармонійного розвитку та задоволення інформаційних потреб особистості; в) гарантування та розвиток інформаційного середовища в інтересах особистості; в) захист від інформаційних загроз.

Об’єктами захисту є стан духовного, психічного та фізичного комфорту особистості, а також умови розвитку усіх сфер її життєдіяльності і суспільства, включно з культурою, наукою, релігією, соціальними зв’язками, психофізичними факторами та мовним середовищем. Інформаційно-психологічна безпека особи та суспільства є складовою інформаційної безпеки держави, визначаючи її політичну специфіку.

Для особистості критичною є цілісність і розвиток свідомості, руйнування яких призводить до втрати соціальної функціональності. Масова свідомість формується через історичний розвиток нації або великої соціальної групи, проте інформаційно-психологічний вплив може її модифікувати. Великі соціальні групи характеризуються стійкими цінностями, нормами поведінки та соціально-психологічними регуляторами, такими як групова свідомість, менталітет, традиції та звичаї. Групова свідомість впливає на

формування типових представників класів, партій або націй, які стають носіями групових норм, цінностей і стереотипів, що враховуються при реалізації інформаційно-психологічного впливу.

Отже, корпоративна та особиста кібербезпека державних службовців є важливою передумовою виникнення парадигмальних зсуви в управління персоналом на державній службі, які формуються у двох вимірах: інформаційно-технічному (впровадження сучасних інформаційних технологій кіберзахисту) та соціально-психологічному (забезпечення психологічної безпеки в кіберпросторі).

Питання взаємодії масмедіа та державної влади все частіше актуалізується в науковому дискурсі міжнародних (Д. Брайант, С. Томпсон, Д. Галлін, П. Манчіні та ін.) та вітчизняних (Х. Буртник, П. Вербицький, А. Костирєв, Ю. Яковенко та ін.) вчених [10; 15; 22; 77; 210]. Традиційно під засобами масової комунікації розуміють сукупність каналів розповсюдження інформації, яку адресовано необмеженому колу осіб, соціальних груп, держав з метою оперативного інформування їх відносно подій і явищ у світі, конкретній країні, певному регіоні, а також для виконання спеціальних соціальних функцій.

Однак, сьогодні не існує єдиного наукового підходу щодо розуміння цілей, ролі, функцій взаємодії масмедіа та державної влади. Так, вчені Д. Брайант, І. Гаврада, С. Томпсон та ін., характеризують взаємодію масмедіа та державної влади в контексті термінологічного ряду «великий арбітр», «голос народу», «четвертий центр влади», «четверта гілка влади», поряд із законодавчою, виконавчою та судовою [218; 227 та ін.]. В їх роботах популяризується віра у всемогутність мас-медіа, а деякі з них наголошують на тому, що «той, хто контролює телебачення, контролює всю країну, тобто має реальну владу в своїх руках» [19].

Інша група вчених (Г. Альтшулл, М. Бурменський, В. Головій О. Сердюк, І. Підкурова та ін.), дотримуються протилежної думки, зокрема вони підкреслюють, що хоч і свідомість людей багато в чому визначається засобами

масової комунікації, це не означає, що масмедія можуть вважатися владним елементом [26]. Інші тези – «…фактично вони тільки слугують розповсюдженню існуючих культурних кодів по готовим формулам, добре відомим медіа-технологам» [12]; «…протягом всієї своєї історії ЗМІ були не більш ніж сліпими літописцями чужих діянь» [201]; «…якщо колись пресі і випадало грати активну роль, то тільки тому, що вона ставала агентом тих чи інших суспільних сил чи політичних рухів [218] – підкреслюють даний підхід. Відомий український вчений Г. Почепцов також є прихильником цієї точки зору і називає мас-медіа основною машиною, що породжує міфи та «створює художні світи» [121].

Важливо акцентувати дослідницьку увагу на дослідженнях, де наводяться відмінні риси масмедія, а саме: публічність (тобто необмежене та надперсональне коло споживачів [Бігнел Д., 227]; наявність спеціальних технічних приладів, апаратури тощо) [Еріксон Дж., 242]; непостійний, дисперсний характер їх аудиторії, що створюється від випадку до випадку в результаті загальної уваги, яка проявилася до того чи іншого засобу передачі інформації [Робінсон Д., 242]; непряма взаємодія комунікаційних партнерів [Ридник В., 310]; моновекторність впливу комунікатора на реципієнта та неможливість зміни їх ролей [315].

На нашу думку, максимально релевантною є погляд теоретика масової комунікації Д. Маккуейла, який відмічає, що медіа можуть розглядатися як:

– вікно (відчинене для подій та досвіду) – коли в процес ніхто не втручається;

– дзеркало подій у суспільстві та у світі – це правдиве відображення, хоча кут зору і напрямок обирають інші;

– фільтр, охоронець – відбір частин інформації для представлення глядачу та затемнення інших (свідомо чи ні);

– гід або перекладач – коли пояснюється те, що на думку комунікатора, глядач не розуміє;

– екран або перешкода – медіа можуть відрізати аудиторію від дійсності, представляючи неправильний погляд на світ [254].

На погляд З. Галаджуна, М. Лашкініної, С. Наумкиної, В. Пилипенко, Ю. Привалова та ін.) основне протиріччя полягає в тому, що масмедія є важливим інститутом громадянського суспільства, що впливає на формування громадської думки, забезпечує інформаційні потреби суспільства та підтримує політичну комунікацію, а державна влада – використовує мас-медіа для поширення інформації про свою діяльність, впливу на громадську думку та реалізації своїх політичних цілей [21; 83; 111].

Отже, можемо констатувати, що на сьогодні основними передумовами парадигмальних зсувів в управлінні персоналом на державній службі є: цифровізація державного сектору; корпоративна та особиста кібербезпека державних службовців; взаємодія масмедіа та державної влади. Саме вони генерують необхідність впровадження комплексних змін у систему державної служби України, зокрема:

– обґрунтування концептуальних засад професійної діяльності державних службовців у кіберпросторі;

– впровадження нової компетентнісної моделі професійної діяльності державних службовців у кіберпросторі;

– модернізація технологій оцінювання готовності кандидатів на зайняття посад державної служби до здійснення професійної діяльності в умовах кіберпростору;

– формування уявлень, цінностей і переконань про те, що цифрова компетентність, професійна мобільність, корпоративна та особиста кібербезпека стають стрижнем кар’єрного розвитку державних службовців.

Висновки з першого розділу

Обґрунтована нами концептуальна модель управління персоналом на державній службі у вимірах взаємодії в кіберпросторі концентрує

дослідницьку увагу на описі ключових термінів, понять, визначень предметної області, а також теоретичних підходів, моделей, методів, інструментів щодо її аналізу.

Кіберпростір – це простір функціонування продуктів інформаційно-комунікаційних технологій, що дозволяють створювати складні системи взаємодій агентів (суб'єкти взаємодії) з метою отримання інформації, обміном та управління нею, а також здійснення комунікацій в умовах великої кількості мереж. Кіберпростір характеризується такими основними ознаками: це інформаційний простір; він є комунікативним середовищем; утворюється за допомогою технічних (комп'ютерних) систем. Кіберпростір має трьохвимірну структуру, складовими якої є фізичні, інформаційні та соціальні компоненти. Особливості взаємодії в кіберпросторі обумовлені феноменами «кібербезпека», «кіберзахист», «кібергігієна», «кіберпсихологічна готовність»,.

Ризики в кіберпросторі охоплюють широкий спектр загроз як для організації (фінансові збитки, порушення конфіденційності даних, втрати репутації тощо), так і окремих осіб (порушення психічного здоров'я, професійне вигорання і т. ін.). Управління ризиками взаємодії в кіберпросторі повинна стани стрижнем HR-стратегій органів публічної влади.

Базовими механізмами взаємодії державних службовців у кіберпросторі є: організаційно-правовий, інформаційно-технічний, соціально-психологічний. Саме через призму розуміння функціонування цих механізмів можна оцінювати ефективність взаємодії державних службовців у кіберпросторі, а також удосконалювати/модернізувати таку взаємодію, під впливом зовнішніх та внутрішніх факторів.

Основними передумовами парадигмальних зсувів в управлінні персоналом на державній службі є: цифровізація державного сектору; корпоративна та особиста кібербезпека державних службовців; взаємодія масмедіа та державної влади. Саме вони генерують необхідність впровадження комплексних змін у систему державної служби України.

РОЗДІЛ 2
СТАН ПРОБЛЕМ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ ДЕРЖАВНИХ СЛУЖБОВЦІВ У КІБЕРПРОСТОРІ

На протилежність теоретичному пізнанню, яке базується на логічних міркуваннях та абстракціях, емпіричному пізнанню притаманні збір фактів, первинне узагальнення, опис дослідних даних, систематизація і класифікація. В контексті даної роботи діяльність дослідника спрямована безпосередньо на об'єкт дослідження, і відбувається на основі методів опитування, порівняння, виміру, аналізу тощо.

Логіка подачі матеріалів другого розділу дисертації корелюється з третім завданням дисертаційного дослідження, яким передбачено визначення стану проблем професійної діяльності державних службовців у кіберпросторі із застосуванням методу соціологічного опитування. Опишемо це детальніше.

2.1. Методика проведення соціологічного опитування державних службовців

Традиційно в науковому дискурсі під методикою розуміється сукупність взаємопов'язаних способів та прийомів доцільного проведення будь-якої роботи [40; 101; 102]. Опис методики проведення соціологічного опитування державних службовців з теми «Стан проблем професійної діяльності державних службовців у кіберпросторі» представимо за такою структурою: мета опитування; теоретико-методологічна база; методи та інструменти проведення опитування; цільова аудиторія (опис виборки); таймінг та етапи виконання робіт.

Так, ***метою опитування*** є виявлення стану проблем професійної діяльності державних службовців у кіберпросторі.

Теоретико-методологічна база. Теоретико-методологічною основою дослідження є положення низки концептуальних підходів, які відображають міждисциплінарний характер аналізу цифрового середовища, професійної діяльності державних службовців та феномену кіберзагроз.

Центральним у розумінні професійної поведінки та реакцій державних службовців у цифровому середовищі є положення «теорії діяльності» О. Леонтьєва, яка акцентує увагу на тому, що розвиток особистості відбувається не лише у межах задоволення базових потреб, але й у процесі творчості та активної діяльності. Важливим аспектом цієї теорії є спрямованість свідомої діяльності людини на досягнення певних цілей, що дозволяє аналізувати поведінку державних службовців у цифровому просторі як результат цілеспрямованої професійної взаємодії та самореалізації.

Для дослідження конфліктогенних ситуацій у кіберпросторі, що негативно впливають на професійну діяльність державних службовців, застосовується положення «загальної теорії конфлікту», представленої у працях Дж. Бернарда, Дж. Доугерті, Р. Пфалтцграффа, Дж. Рубіна, Д. Прютта та С. Кима. Ця теорія узагальнює емпіричні знання з проблем напруженості, конфліктів та конкуренції, накопичені у різних соціально-гуманітарних науках, і дозволяє інтерпретувати кіберхейт як специфічний тип соціального конфлікту, що трансформується у цифровому просторі.

Додатково, методологічною опорою є положення теорії соціальної підтримки (H. Cobb, S. Cohen, L. Berkman), яка визначає вплив соціальних мереж, груп підтримки та інституційних механізмів на подолання стресових ситуацій і адаптацію людини до несприятливих умов. Цей підхід є ключовим для аналізу впливу онлайн-середовища на психологічне самопочуття державних службовців та пошуку шляхів організації підтримки у випадках переживання кіберзагроз.

У контексті цифровізації діяльності державних органів значущою є також теорія інформаційного суспільства (М. Кастельс, Д. Белл), яка дозволяє пояснити зростання ролі інформаційних технологій у професійній діяльності

та у житті суспільства загалом, а також пов’язані з цим ризики цифрової вразливості, зокрема зростання кіберзлочинності та поширення ненависті в мережі.

Застосування міждисциплінарної теоретико-методологічної бази дозволяє комплексно розглядати не лише поведінкові, але й психологічні, соціальні та управлінські аспекти взаємодії державних службовців з цифровим середовищем, а також розробити ефективні інструменти підтримки їхньої діяльності у вимірах кіберпростору.

Методи та інструменти проведення опитування. Інструментарій дослідження, як правило, прив’язується до основного методу дослідження. В контексті цієї роботи – це метод опитування з використанням спеціально розробленої онлайн-анкети. Опитування здійснювалося серед державних службовців України та мало на меті зібрати емпіричні дані щодо особливостей цифрової поведінки, рівня обізнаності, досвіду зіткнення з негативними явищами у віртуальному середовищі, зокрема кіберхейтом, а також ставлення до них і вироблених стратегій реагування.

Обраний метод дозволив забезпечити широту охоплення респондентів, збереження анонімності та конфіденційності відповідей, що є надзвичайно важливим з огляду на чутливість тематики дослідження. Анкета була розроблена спільно з командою експертів міжнародного проєкту DAAD-2024 № 57709682 «Навігація у цифровому просторі: стратегії підтримки з урахуванням конфліктів» із врахуванням міжнародного досвіду дослідження явищ онлайн-дискримінації та цифрової безпеки (див. Додаток Б).

Усі запитання анкети було структуровано за тематичними блоками з метою поетапного виявлення особистісних характеристик респондентів, особливостей їхнього професійного середовища, рівня взаємодії у цифровому просторі, а також досвіду та ставлення до онлайн-ненависті. Методика побудована таким чином, щоб поєднувати як кількісні, так і якісні елементи аналізу.

Для збору інформації використовувалися переважно закриті питання (одно- та багатоваріантні), шкальні питання типу Лайкерта, питання з частотними шкалами, а також окремі відкриті запитання для отримання більш гнучких та змістовних відповідей. Це дозволяє не лише кількісно оцінити поширеність тих чи інших явищ, але й якісно дослідити суб'єктивні реакції, мотивації та соціальні контексти поведінки державних службовців у цифровому середовищі.

Анкета складається з кількох змістовних блоків, що дозволяють комплексно охопити різні аспекти професійного та особистого функціонування державних службовців у кіберпросторі. Вона включає як питання соціально-демографічного характеру, так і спеціалізовані питання, що стосуються онлайн-поведінки, досвіду кіберхейту та механізмів реагування на такі ситуації.

Перший блок спрямований на збирання загальної соціально-демографічної інформації про респондентів: вік, стать, мову спілкування, тип населеного пункту проживання та інформацію про перебування в зоні конфлікту. Цей блок дозволяє дослідити можливі соціокультурні фактори, що впливають на досвід та сприйняття кіберпростору.

Другий блок містить питання, які оцінюють особистісні характеристики респондентів, зокрема рівень самооцінки, емоційний стан, здатність до самопідтримки та сприйняття власної ефективності. Для цього використано шкальні питання з п’ятиступеневою градацією відповідей, що дозволяє виявити рівень психологічної стійкості та самовизначення державних службовців.

Третій блок присвячено аналізу якості соціальної взаємодії в професійному середовищі, зокрема комунікації з колегами та рівня довіри до різних соціальних інститутів: органів влади, керівництва, політиків, ЗМІ тощо. Це дозволяє оцінити соціальний капітал державних службовців та потенційний рівень підтримки у випадках проявів кібербулінгу.

Четвертий блок зосереджено на вивченні цифрової поведінки

респондентів, зокрема частоти використання різних соціальних мереж та месенджерів, а також оцінки власної схильності до інтернет-залежності, до прокрастинації. Це дає змогу з’ясувати інтенсивність присутності в кіберпросторі та потенційні ризики.

П’ятий блок містить комплекс питань, що безпосередньо стосуються досвіду спостереження та особистого переживання кіберхейту. Окрім визначення частоти та місць виникнення онлайн-ненависті, увага приділяється її тематиці: етнічна, релігійна, політична, гендерна чи інші види дискримінації. Особливістю цього блоку є оцінка як емоційних реакцій респондентів на кіберхейт, так і реальних дій, які вони здійснюють у відповідь на такі ситуації (ігнорування, звернення по допомогу, технічні заходи тощо).

Шостий блок стосується саморефлексії респондентів щодо власної поведінки в Інтернеті. Зокрема, досліджується потенційна участь самих державних службовців у поширенні образливого контенту, а також мотиваційні чинники, що можуть спонукати до такої поведінки.

Сьомий блок присвячено вивченню системи соціальної підтримки у випадках переживання онлайн-ненависті. У ньому респонденти зазначають, до кого вони звертаються по допомогу або підтримку (родичі, колеги, керівництво, психологи, поліція) та яку саме допомогу вважають для себе бажаною. Завершується анкета питанням про те, чи розглядалася тема кіберхейту у робочому середовищі респондентів.

Таким чином, запропонована анкета є багатовимірним інструментом, що дозволяє не лише виявити ступінь поширеності кіберзагроз серед державних службовців, а й проаналізувати психологічні, соціальні та поведінкові аспекти їхньої діяльності у цифровому просторі. Структура анкети забезпечує отримання даних, необхідних як для кількісного, так і для якісного аналізу, що відповідає вимогам сучасних соціогуманітарних досліджень у сфері державного управління.

На основі Google-форми було створено електронну версію анкети, структурованої за тематичними блоками, що охоплюють соціально-

демографічні характеристики, рівень особистісної самооцінки, соціальну взаємодію, цифрову поведінку, досвід кіберзагроз і стратегії реагування. Її зміст орієнтований на поєднання кількісного та якісного аналізу й адаптований до сучасних вимог соціогуманітарних досліджень.

Отримані дані були піддані математичній та статистичній обробці для визначення достовірності міжгрупових відмінностей, виявлення закономірностей та взаємозв'язків між показниками. Аналіз здійснювався з використанням програмного забезпечення SPSS 21, STATISTICA 8.0 і Microsoft Excel.

Зважаючи на результати перевірки нормальності розподілу, було виявлено відхилення від нормального розподілу деяких змінних. У зв'язку з цим у дослідженні застосовувалися непараметричні методи аналізу, зокрема:

U-критерій Манна-Уітні – для порівняння незалежних вибірок;

H-критерій Краскела-Уоліса – для порівняння трьох і більше груп;

коефіцієнт кореляції Пірсона (r) – для виявлення зв'язків між кількісними змінними.

Опрацювання результатів включало як кількісний аналіз (відсотковий розподіл, частотність, середні значення), так і якісну інтерпретацію суб'єктивних оцінок респондентів. Це дало змогу комплексно охарактеризувати психологічні, поведінкові та організаційні особливості професійної діяльності державних службовців у цифровому середовищі.

Детальні результати обробки та аналізу даних подані в наступних підрозділах розділу.

Поєднання опитування з іншими методами дозволило значно знизити вихідний суб'єктивізм отриманих даних, а також підвищити валідність і надійність застосованого опитувальника/анкети.

Цільова аудиторія (опис вибірки). Загальна кількість учасників опитування склала 4684 особи. Гендерний розподіл респондентів був таким: 40,1% опитаних становили жінки, а 59,9% – чоловіки (рис. 2.1). Таким чином, вибірка репрезентує обидві статі, з незначним переважанням чоловіків.

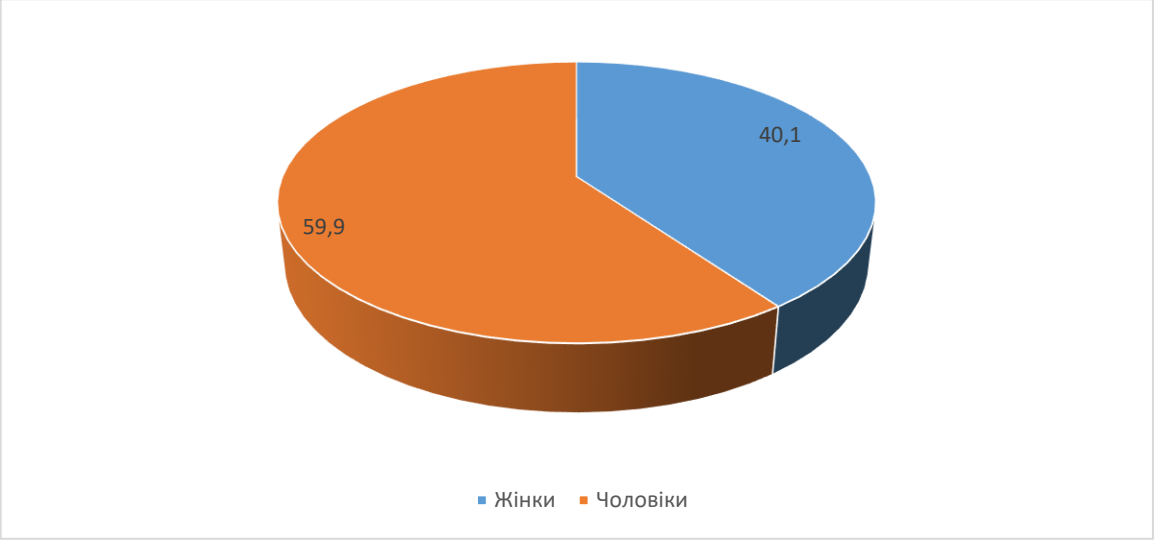

Рис. 2.1. Розподіл респондентів за ґендерною ознакою

Віковий склад респондентів охоплював осіб віком від 22 до 67 років, що дозволяє досліджувати досвід взаємодії з цифровим середовищем як молодших, так і старших державних службовців. Середній вік учасників склав M = 44,5 років при стандартному відхиленні SD = 13,28 років, що вказує на варіативність вікової структури вибірки.

За місцем проживання більшість респондентів (73,3%) проживають у міській місцевості, 18,4% – у передмісті, і лише 8,3% мешкають у сільській місцевості (рис. 2.2). Такий розподіл дозволяє відобразити специфіку взаємодії з цифровими технологіями у різних типах населених пунктів.

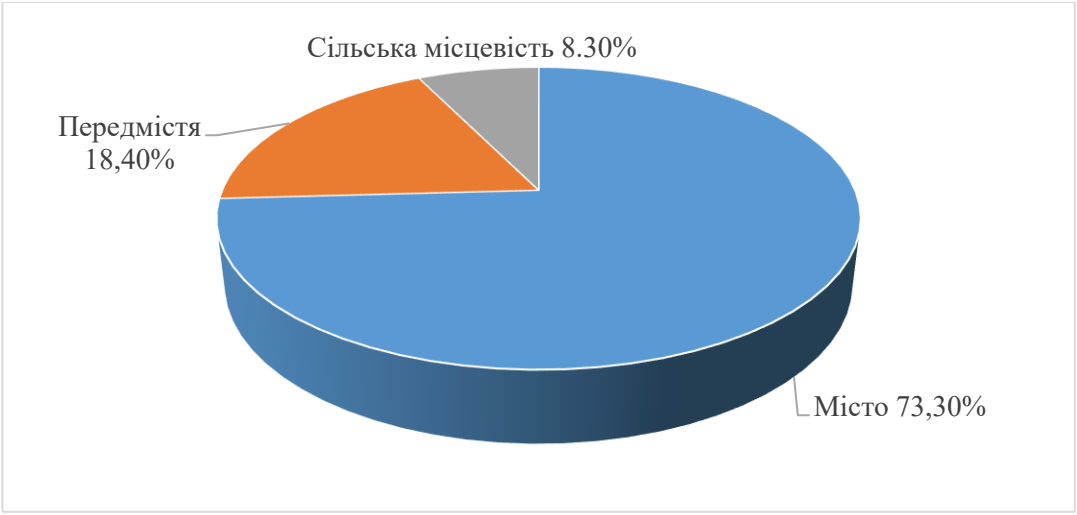

Рис. 2.2. Розподіл респондентів за місцем проживання

Значущим є також контекст безпекової ситуації: 40,4% учасників опитування зазначили, що проживають у зоні конфлікту, що може мати безпосередній вплив на їхній емоційний стан, активність у кіберпросторі та сприйняття цифрових ризиків (рис. 2.3).

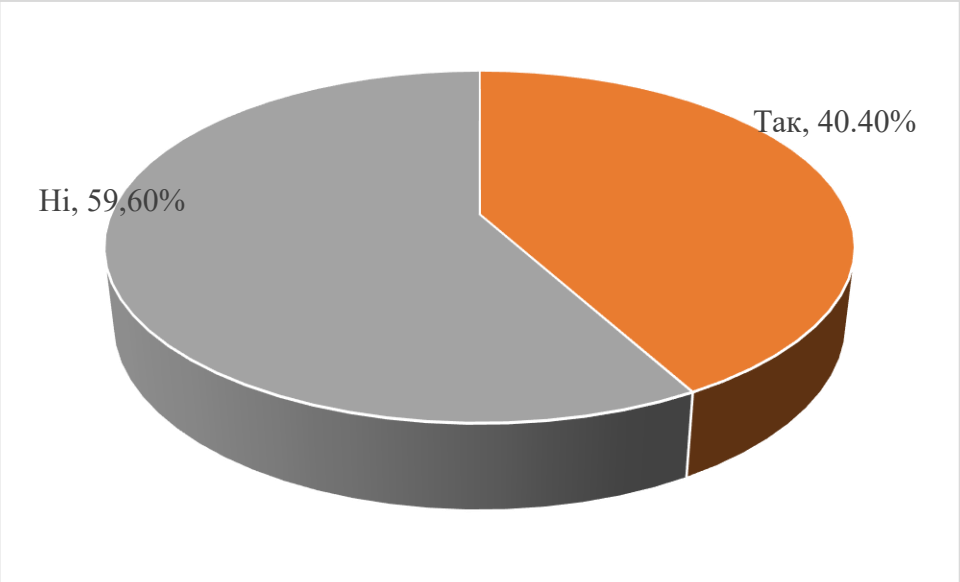

Рис. 2.3. Розподіл респондентів щодо знаходження місця проживання у зоні конфлікту

Щодо мовного розподілу, 69,1% опитаних зазначили, що спілкуються українською мовою, 24,3% – російською, ще 6,6% респондентів вказали інші мови (рис. 2.4). Це вказує на мовну та культурну різноманітність аудиторії, яка також може впливати на особливості комунікації у цифровому середовищі.

Рис. 2.4. Розподіл респондентів за носіями рідної мови

Таким чином, вибірка є достатньо великою, гендерно та соціально диференційованою, охоплює різні вікові групи, територіальні особливості проживання та мовні ідентичності, що створює надійну емпіричну основу для аналізу стану проблем професійної діяльності державних службовців у вимірах кіберпростору.

Таймінг та етапи виконання робіт. Дослідження проводилося протягом 2024 року в три етапи:

на першому етапі – здійснювалася розробка теоретико-методологічних засад дослідження, формування концептуального апарату та створення онлайн-анкети для опитування. Особлива увага приділялася міждисциплінарному підходу до розробки інструментарію, узгодженню термінології та адаптації міжнародного досвіду до українських реалій. Анкета проходила апробацію на експертній групі з метою забезпечення її валідності та надійності.

на другому – було організовано та проведено онлайн-опитування державних службовців. Було налагоджено комунікацію з потенційними учасниками дослідження через професійні спільноти, офіційні канали державних установ, електронні розсилки та соціальні мережі. Сам процес збору даних забезпечував повну анонімність та добровільність участі.

на третьому – проводилася обробка отриманих даних, їх статистичний аналіз та інтерпретація результатів з урахуванням теоретичних положень дослідження. Отримані емпіричні дані стали основою для формулювання висновків щодо стану проблем професійної діяльності державних службовців у кіберпросторі, а також для напрацювання рекомендацій з удосконалення політик цифрової безпеки та підтримки персоналу в умовах сучасних кіберзагроз.

Таким чином, послідовна реалізація зазначених етапів забезпечила цілісність, наукову обґрунтованість та достовірність проведеного соціологічного дослідження.

2.2. Характеристика стану готовності державних службовців до професійної діяльності в кіберпросторі

Проведене соціологічне опитування дає змогу комплексно оцінити рівень обізнаності державних службовців щодо цифрового середовища, їхню готовність протидіяти кіберризикам, а також виявити специфіку їхньої взаємодії з кіберпростором. Отримані результати дозволяють здійснити всебічний аналіз ключових тенденцій, проблемних аспектів та актуальних потреб у сфері цифрової безпеки й професійної адаптації. Крім того, дослідження охоплює питання самооцінки респондентів та рівня довіри до найближчого соціального й професійного оточення, що дає змогу виявити низку психологічних і соціальних чинників, які безпосередньо впливають на їхній стан готовності до ефективної професійної діяльності в умовах цифрового середовища.

Так, аналіз самооцінки державних службовців за результатами соціологічного опитування, відображений у табл. 2.1, дозволяє охарактеризувати особливості їхнього психологічного самосприйняття, рівень внутрішньої впевненості, емоційної стабільності та загального ставлення до себе в контексті професійної діяльності в кіберпросторі.

Загальний аналіз відповідей свідчить про внутрішню суперечливість самооцінки значної частини державних службовців. Попри те, що позитивні судження про власні якості й можливості (наприклад, «Я здатний дещо робити не гірше, ніж більшість» – 47,7% погоджуються; «Я відчуваю, що я гідна людина...» – 57,9%) є досить поширеними, водночас спостерігається виражена схильність до самокритики та емоційної нестабільності. Так, 67,9% респондентів згодні з твердженням «Іноді я відчуваю свою неефективність», а 47,8% визнають, що іноді вважають себе невдахами.

Крім того, майже половина опитаних (40,3%) прагне більшої самоповаги, а 53,7% відчувають, що «особливо немає чим пишатися», що

свідчить про дещо занижену оцінку власної значущості в професійному середовищі або вплив тривалого стресу та негативного інформаційного фону.

Таблиця 2.1

Самооцінка державних службовців (%).

	абсолютно не згоден	**не згоден**	**важко відповісти**	**згоден**	**повністю згоден**
Загалом я задоволений(на) собою	20,9	29,7	12,6	19,5	17,3
Іноді я думаю, що я у всьому поганий(на)	16,4	21,3	14,6	28,4	19,3
Мені здається, що в мене є низка хороших якостей	14,3	22,4	13,6	28,6	21,1
Я здатний дещо робити не гірше, ніж більшість	13,7	19,7	18,9	26,9	20,8
Мені здається, що мені особливо немає чим пишатися	13,2	17,8	15,3	30,2	23,5
Іноді я відчуваю свою неефективність	9,5	11,4	11,2	35,2	32,7
Я відчуваю, що я гідна людина, принаймні не менше за інших	11,8	10,9	19,4	30,5	27,4
Мені хотілося б більше поважати себе	19,5	22,4	17,8	21,6	18,7
Я завжди схильний/схильна почуватися невдахою	17,4	19,5	15,3	24,5	23,3
Я до себе добре ставлюся	14,7	18,6	16,9	26,7	23,1
Я дуже скептична людина і ставлюся до всього з обережністю та увагою	10,4	15,1	16,5	29,9	28,1

Показово, що лише 36,8% респондентів повністю або частково погоджуються з твердженням «Загалом я задоволений(на) собою», тоді як 50,6% мають протилежну думку. Це може бути індикатором високого рівня внутрішнього критицизму або наслідком емоційного вигорання на державній службі, особливо в умовах інформаційних перевантажень, які характерні для кіберпростору.

Варто також звернути увагу на високий рівень саморефлексії й емоційної чутливості респондентів: значна частка державних службовців

відзначає, що схильні розмірковувати про себе, свої дії, моральні орієнтири (рис. 2.5.).

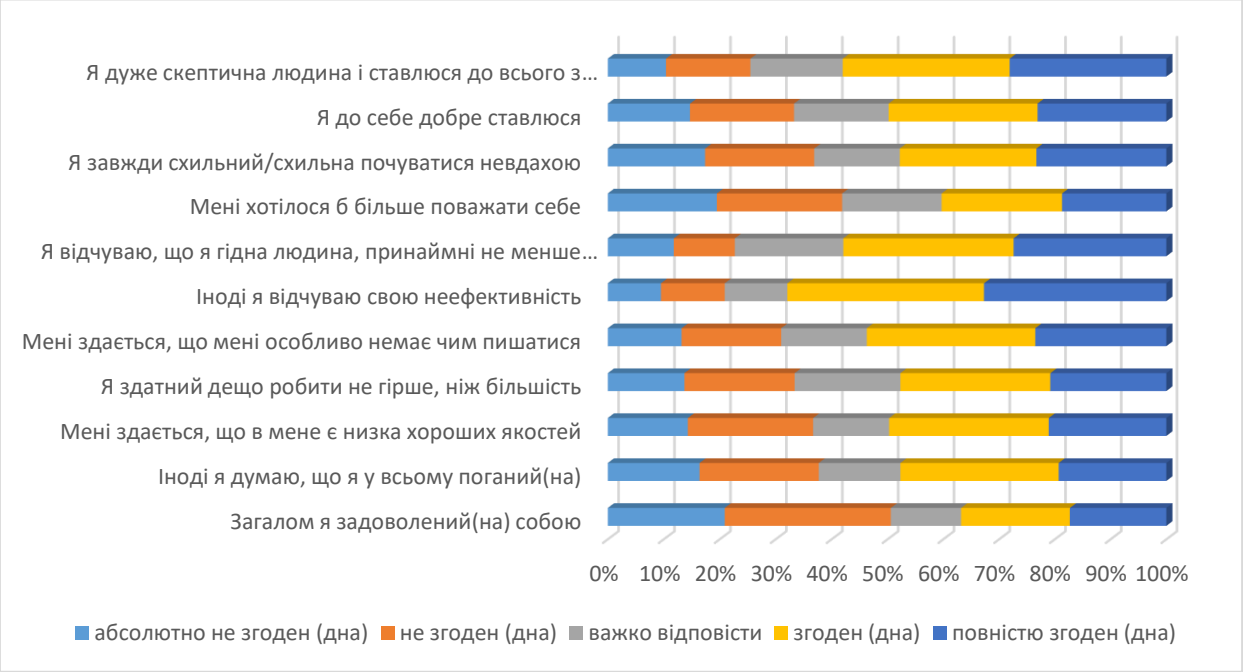

Рис. 2.5. Рівень саморефлексії й емоційної чутливості державних службовців (%).

Таким чином, отримані результати дозволяють констатувати неоднорідний рівень самооцінки, де поєднуються прояви впевненості з ознаками внутрішньої уразливості, що має бути враховано під час розробки програм підтримки психоемоційного добробуту державних службовців в умовах цифрової взаємодії. Також це свідчить про потенціал для розвитку етичного самоуправління, однак водночас вказує на потребу в психологічній підтримці та тренінгах із розвитку стресостійкості, емоційного інтелекту та самоцінності.

Аналіз даних, наведених у табл. 2.2, дозволяє оцінити якість міжособистісної взаємодії державних службовців із колегами, яка є важливим чинником не лише психологічного комфорту, а й ефективності командної роботи, комунікаційної відкритості та стресостійкості працівників у цифровому середовищі.

Таблиця 2.2

Міжособистісна взаємодія державних службовців із колегами (%).

	абсолютно не згоден	**не згоден**	**важко відповісти**	**згоден**	**повністю згоден**
Я можу обговорювати свої погляди з кимось із колег, не відчуваючи при цьому скутості чи збентеження	30,7	33,8	12,5	12,1	10,9
Мої колеги завжди уважно слухають мене	30,4	34,2	13,4	11,8	10,2
Я дуже задоволений тим, як ми з колегами спілкуємося	28,9	35,2	15,6	10,8	9,5
Якби в мене були неприємності, я міг би розповісти про це колегам	32,4	36,5	14,2	10,6	6,3

Аналіз таблиці свідчить про високий рівень комунікативної відчуженості та соціальної замкненості, що переважає у професійному середовищі державних службовців. За всіма твердженнями понад 60% респондентів (у деяких випадках – до 69%) не погоджуються з позитивними характеристиками комунікації з колегами. Наприклад, 64,5% не погоджуються з тим, що можуть вільно висловлювати свої погляди без збентеження, 64,6% – з тим, що їх уважно слухають колеги, а 64,1% не задоволені спілкуванням у колективі.

Особливо тривожним є те, що лише 16,9% опитаних вважають, що у разі проблем могли б поділитися цим із колегами, тоді як 68,9% цього не припускають. Це вказує на дефіцит довіри та емоційної підтримки у робочому колективі, що може ускладнювати процеси адаптації, спільного прийняття рішень, обговорення конфліктних ситуацій, а також посилювати почуття ізоляції, зокрема у кризових ситуаціях чи під час перебування в кіберпросторі.

Невисокий відсоток респондентів, які відзначають задоволення якістю спілкування на роботі (лише 20,3% у сукупності «згоден» і «повністю згоден»), свідчить про недостатньо розвинені горизонтальні комунікаційні зв’язки, які є важливими для формування згуртованого професійного середовища (рис. 2.6.).

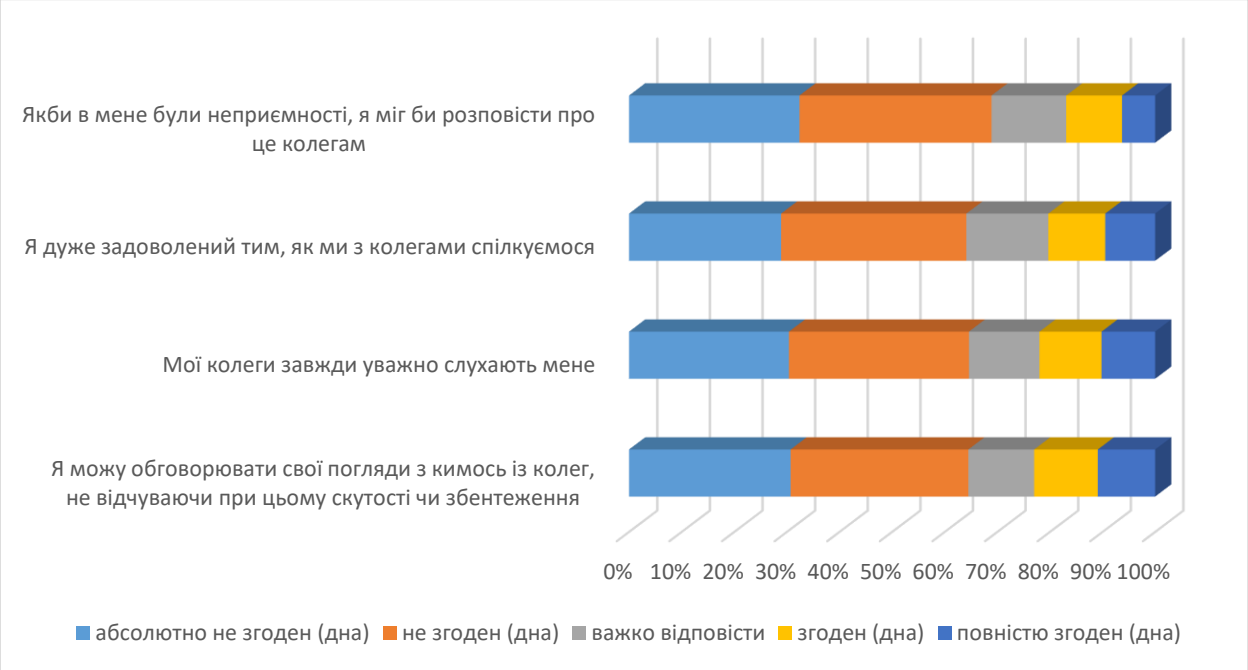

Рис. 2.6. Якість міжособистісної взаємодії державних службовців із колегами (%).

Таким чином, отримані результати свідчать про необхідність цілеспрямованої роботи з формування позитивного мікроклімату в колективах державної служби, зокрема через командні тренінги, розвиток комунікативних навичок, системи менторства та заходи з підвищення емоційного інтелекту в умовах цифрового середовища. Це важливо також з урахуванням зростаючої ролі кіберпростору, де відсутність підтримки з боку колег може поглиблювати вплив кіберзагроз на психологічне здоров'я службовців.

Аналіз результатів соціологічного опитування щодо рівня довіри державних службовців до різних інституцій та соціального оточення (табл. 2.3) дозволяє оцінити соціальну довіру як компонент професійної готовності та стійкості до викликів у цифровому середовищі.

Найвищий рівень довіри серед державних службовців, згідно з результатами опитування, зафіксовано до колег по роботі: 46,9% респондентів зазначили, що принаймні частково або повністю довіряють своїм колегам, що створює певний потенціал для формування горизонтальних комунікацій і

командної взаємодії. Разом із тим, 27,5% прямо висловили недовіру, а ще чверть респондентів не змогли визначитися з відповіддю.

Таблиця 2.3

Стан довіри державних службовців до оточення (%).

	я не довіряю	**я не впевнений**	**я трохи довіряю**	**я дуже довіряю**
Президент	32,9	26,7	21,2	19,2
Мій керівник/моє керівництво	28,6	36,8	21,2	13,4
Політики	38,7	37,9	13,2	10,2
Мої колеги	27,5	25,6	25,8	21,1
Поліція	31,2	32,8	24,5	11,5
Закон/правова система	34,8	37,3	15,4	12,5
Засоби масової інформації	42,9	39,6	14,3	3,2

Довіра до керівництва установи є суттєво нижчою: лише 34,6% (сума тих, хто трохи або дуже довіряє) схильні довіряти своїм безпосереднім керівникам. Натомість 28,6% заявили про недовіру, а найбільша частка – 36,8% – не впевнені у своїй позиції, що свідчить про невизначеність та можливу напругу у вертикальних службових відносинах.

Рівень довіри до державних інститутів загалом демонструє стійку кризу довіри. Так, президенту не довіряють 32,9% опитаних, поліції – 31,2%, а законодавчій та судовій системі – 34,8%. Ще вищий рівень недовіри спостерігається до політиків загалом (38,7%) та засобів масової інформації — 42,9%. При цьому лише 3,2% респондентів висловлюють повну довіру до ЗМІ, що може свідчити про дефіцит якісної, об’єктивної інформації та високий рівень інформаційного скептицизму серед державних службовців.

Сукупно ці результати засвідчують низький рівень інституційної довіри, що становить потенційний ризик для ефективної реалізації політик, пов’язаних із цифровою безпекою, комунікаційною відкритістю та реагуванням на випадки кіберзагроз (рис. 2.7). Така ситуація також може знижувати готовність службовців звертатися за допомогою чи повідомляти про прояви кібербулінгу та кіберхейту до офіційних структур, зокрема поліції, керівництва чи медіа.

Таким чином, результати опитування вказують на необхідність посилення інституційної комунікації, підвищення прозорості управлінських процесів, а також розвитку програм зміцнення довіри між державними службовцями та ключовими суспільними інститутами.

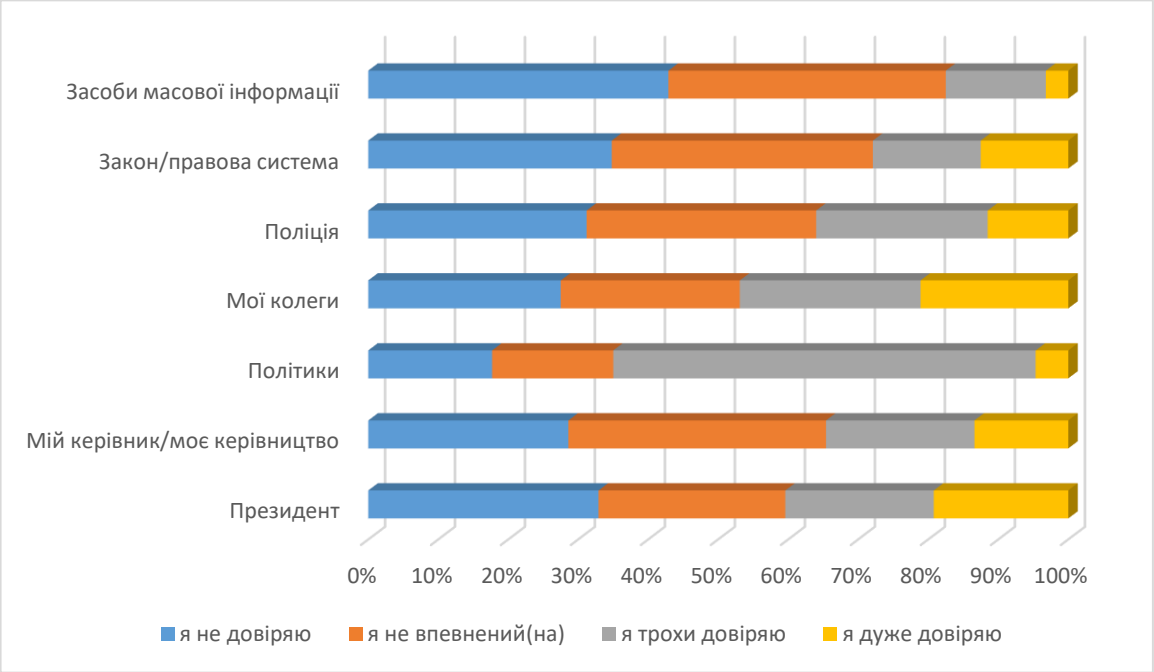

Рис. 2.7. Рівень довіри державних службовців до різних інституцій та соціального оточення, %.

З метою з'ясування ступеня цифрової залученості державних службовців, було поставлено питання: «Скільки часу Ви проводите в Інтернеті в робочий час?». Отримані відповіді свідчать про високу інтенсивність використання Інтернету в межах професійної діяльності, що, з одного боку, демонструє діджиталізацію управлінських процесів, а з іншого – може вказувати на ризики цифрового перевантаження або нецільового використання робочого часу.

Зокрема, лише 8,9% респондентів зазначили, що проводять в Інтернеті до 30 хвилин на день, що може бути ознакою обмеженої цифрової активності або специфіки виконуваних функцій, які не передбачають активного онлайн-взаємодії. 37,6% опитаних вказали, що перебувають в Інтернеті від 3 до 5

годин, а ще 31,2% – понад 5 годин щоденно, що свідчить про майже повну цифрову інтеграцію їхньої професійної діяльності у мережеве середовище. При цьому 22,3% користуються мережею 1-3 години щодня, що можна вважати відносно помірним показником (рис. 2.8).

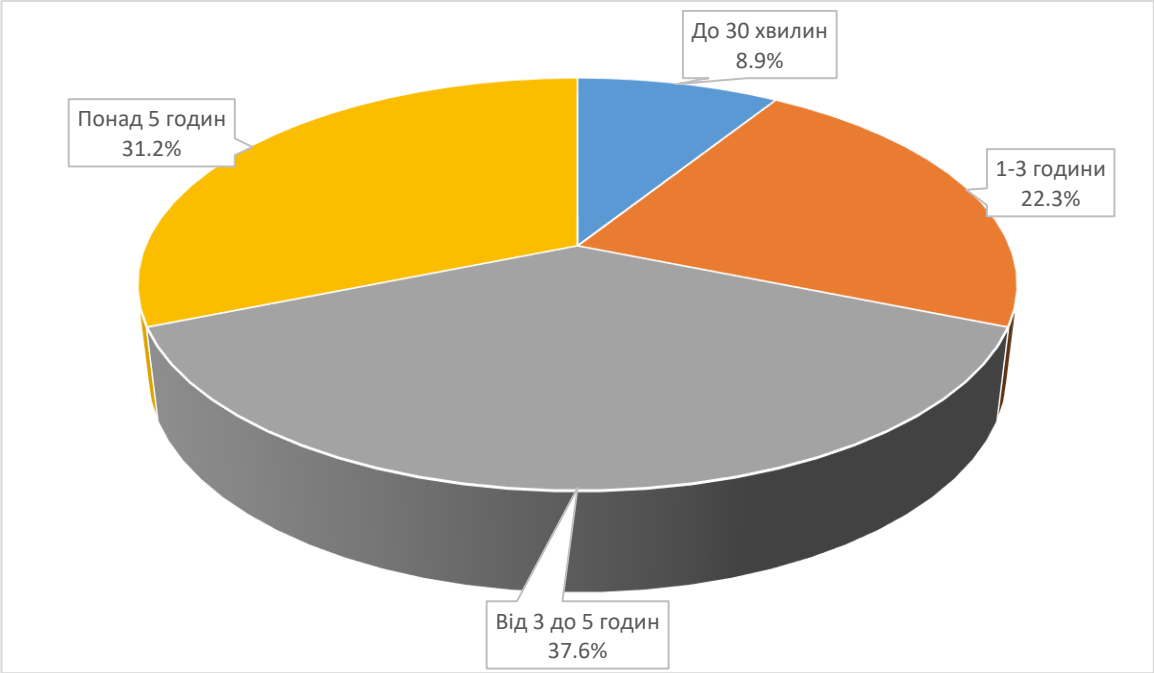

Рис. 2.8. Розподіл респондентів за проведеним часом в Інтернеті (%).

Такий розподіл відповідей відображає тенденцію до зростання цифрової залежності службовців у процесі виконання посадових обов'язків, водночас висвітлюючи потенційні зони ризику – зокрема, професійну прокрастинацію, інформаційне перенасичення, а також розмитість межі між особистим і робочим онлайн-простором.

Зазначені результати актуалізують необхідність впровадження внутрішніх стандартів цифрової гігієни, тайм-менеджменту та саморегуляції у професійному середовищі публічної служби.

Одним із ключових аспектів цифрової взаємодії є баланс між професійною концентрацією та впливом неслужбових онлайн-активностей під час робочого часу. Для виявлення реального стану цієї динаміки серед державних службовців було проаналізовано два показники: відволікання на неслужбовий контент та цифрову прокрастинацію.

Щодо частоти відволікань на неслужбові онлайн-активності (перегляд соціальних мереж, приватне листування, споживання розважального контенту тощо), лише 4,6% респондентів заявили, що ніколи не займаються такими діями під час виконання службових обов'язків. Ще 5,5% роблять це рідко (раз на тиждень або рідше). Водночас, 28,7% учасників зазначили, що відволікаються іноді (декілька разів на тиждень), 41,3% – часто (щодня або майже щодня), а 19,9% – постійно, тобто протягом більшої частини робочого дня. Таким чином, сукупно понад 60% респондентів у тій чи іншій формі визнають систематичне переключення уваги на неслужбовий контент, що створює ризики зниження ефективності публічного управління, втрати робочого часу та розфокусованості в управлінських процесах (рис. 2.9).

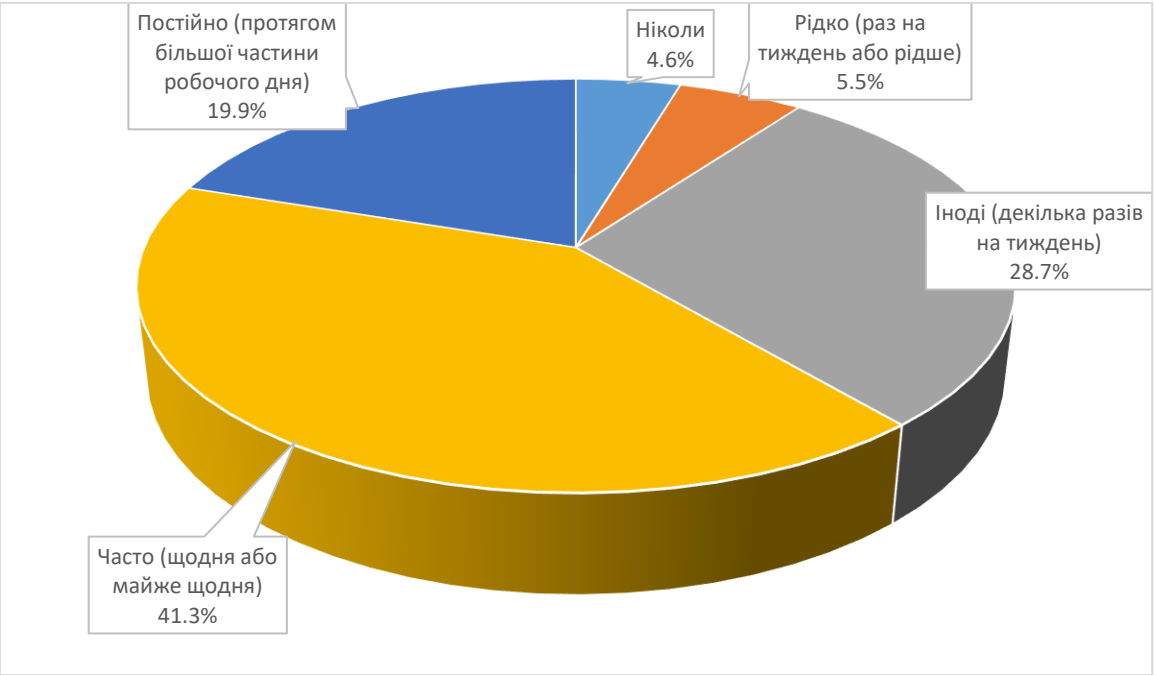

Рис. 2.9. Частота відволікань державних службовців на неслужбовий контент (%).

Другий вектор аналізу – цифрова прокрастинація, тобто схильність відкладати виконання професійних завдань або прийняття рішень, переключаючись на другорядну або незначущу цифрову активність (перевірка новин, соцмереж, відео тощо). Лише 10,8% респондентів зазначили, що ніколи не стикаються з таким явищем, а 11,5% – що це трапляється рідко. Водночас

31,2% службовців зізналися, що іноді (декілька разів на тиждень) відкладають роботу задля таких активностей, ще 24,7% – роблять це майже щодня, а 21,8% – дуже часто, майже постійно (рис. 2.10).

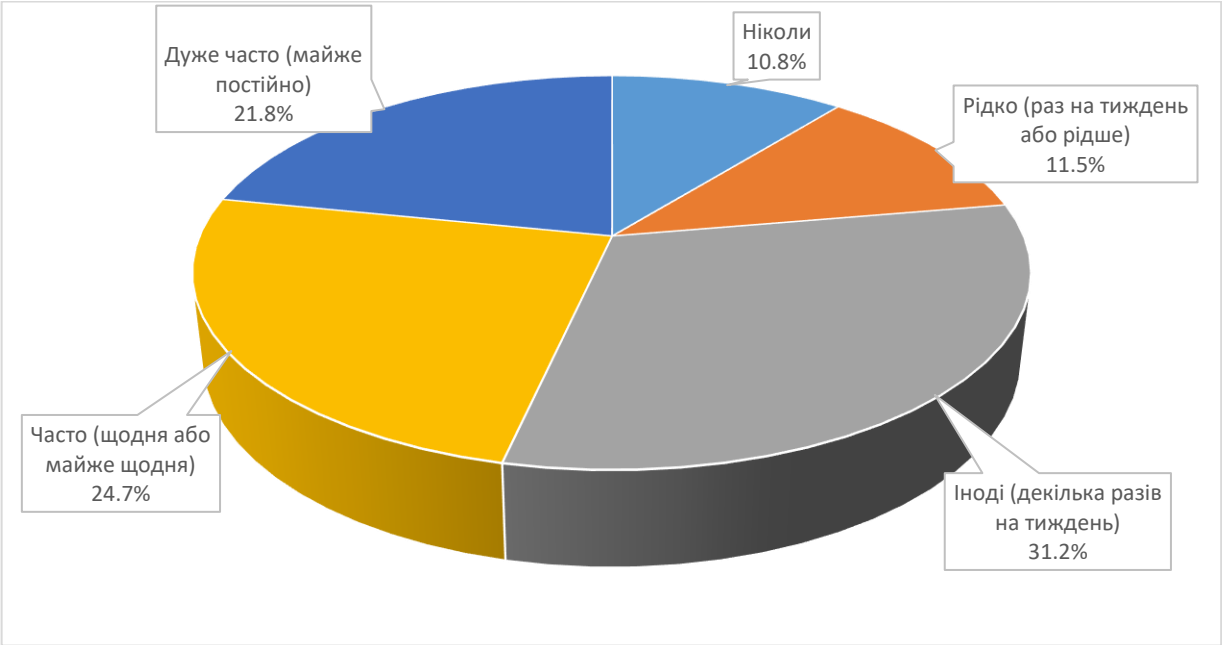

Рис. 2.10. Цифрова прокрастинація серед державних службовців (%).

Сукупно понад три чверті опитаних (77,7%) підтвердили, що схильні до прокрастинаційної поведінки в цифровому середовищі, що є тривожним сигналом у контексті раціонального використання робочого часу в публічному секторі.

Отримані дані дозволяють стверджувати, що підвищена цифрова навантаженість, відсутність чітких меж між професійною та особистою онлайн-активністю, а також брак цифрової саморегуляції можуть істотно впливати на рівень організаційної ефективності та професійної дисципліни серед державних службовців. Це обґрунтовує потребу у впровадженні цифрової гігієни, інформаційного тайм-менеджменту та розвитку компетенцій самоконтролю в умовах кіберпростору.

Дані, представлені в табл. 2.4, ілюструють частотність окремих моделей поведінки державних службовців у цифровому середовищі протягом останнього року. Особлива увага приділяється аспектам надмірного або неконтрольованого використання Інтернету, що може бути маркером

цифрової залежності, емоційної вразливості чи втрати продуктивності в професійній діяльності.

Таблиця 2.4

Користування інтернетом державними службовцями (%).

	ніколи	**кілька разів**	**принаймні щотижня**	**щодня або майже щодня**
Я не їв(ла) і не спав(ла) через Інтернет	21,9	33,5	26,3	18,3
Я відчував(ла) роздратування, коли не міг(могла) зайти в Інтернет	13,4	34,4	32,4	19,8
Я виявив(ла), що користуюся Інтернетом, навіть якщо він мене не дуже цікавить	10,9	33,8	34,1	21,2
Через час, проведений в Інтернеті, я приділяю менше часу сім'ї, друзям чи роботі, ніж варто було б	7,8	25,5	31,1	35,6
Я безуспішно намагався(лася) проводити менше часу в Інтернеті	5,6	21,2	34,5	38,7

Найвищі показники щоденного або майже щоденного повторення мають ті твердження, які вказують на усвідомлення цифрової перевантаженості та спроби її подолання. Так, 38,7% респондентів зізналися, що безуспішно намагалися зменшити тривалість перебування в Інтернеті, що свідчить про наявність певного ступеня залежності. Ще 34,5% вказали, що такі спроби були регулярними хоча б раз на тиждень.

Понад третина державних службовців (35,6%) щодня або майже щодня відзначають, що через надмірне перебування в мережі не приділяють достатньо уваги своїй родині, друзям або професійним обов’язкам, а ще 31,1% стикаються з цією проблемою щотижнево. Таким чином, майже дві третини респондентів визнають, що цифрове навантаження має негативний вплив на баланс між особистим і професійним життям.

Також значна частка респондентів (21,2% – щодня або майже щодня, 34,1% – принаймні щотижня) визнає, що користується Інтернетом навіть за

відсутності реальної потреби чи інтересу до вмісту, що може вказувати на явища прокрастинації та автоматизованої поведінки в онлайн-середовищі.

Реакція на неможливість доступу до мережі також демонструє тривожні симптоми: 19,8% службовців часто відчувають роздратування через обмеження доступу до Інтернету, ще 32,4% – принаймні щотижня. Це може свідчити про психологічну залежність та зниження цифрової гігієни.

Найменше поширеним, але все ж суттєвим, виявився симптом порушення базових фізіологічних потреб унаслідок онлайн-активності: 18,3% респондентів зізналися, що щоденно або майже щоденно пропускають прийоми їжі або сон через користування Інтернетом, ще 26,3% – роблять це щотижнево. Таким чином, сукупно майже 45% державних службовців у тій чи іншій мірі нехтують фізіологічними потребами через цифрову активність.

Загалом результати свідчать про високий рівень інтегрованості цифрових практик у повсякденну діяльність державних службовців (рис. 2.11), що потребує подальшої уваги з боку органів державної влади щодо формування навичок саморегуляції в інформаційному середовищі, збереження продуктивності та запобігання негативним психологічним наслідкам надмірного перебування в Інтернеті.

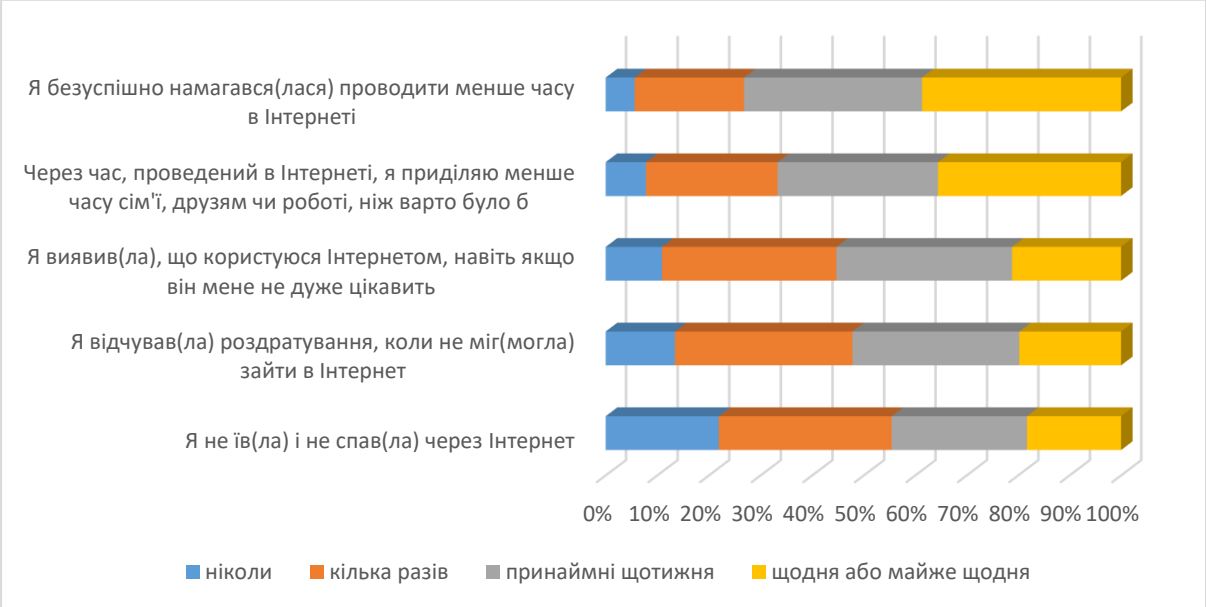

Рис. 2.11. Частота використання Інтернету державними службовцями (%.

Результати соціологічного опитування свідчать про широку залученість державних службовців до цифрових комунікацій через соціальні мережі та месенджери, що підтверджує актуальність дослідження їхньої присутності в кіберпросторі та пов'язаних з цим ризиків. У табл. 2.5 подано частотний розподіл за часом щоденного користування ключовими цифровими платформами.

Таблиця 2.5

Найбільш поширені соціальні мережі серед державних службовців (%).

	ніколи	**менше 2 годин на день**	**2-4 години на день**	**більше 4 годин на день**
Tik-Tok	18,5	13,1	26,7	41,7
Twitch	55,6	12,3	31,6	0,5
YouTube	8,1	14,1	34,1	43,7
Online Messenger: WhatsApp, Telegram, Signal	16,3	18,1	25,2	40,4
Twitter / X	68,8	16,3	14,1	0,8
Instagram	33,4	20,1	22,0	24,5
Facebook	22,6	22,0	27,1	28,3
Discord	80,1	8,2	11,5	0,2
Viber	8,9	17,3	31,3	42,5

Найбільш активно використовуваними серед респондентів виявилися YouTube, Viber, TikTok та онлайн-месенджери (WhatsApp, Telegram, Signal). Зокрема, 43,7% опитаних повідомили, що проводять на YouTube понад 4 години щодня, ще 34,1% – від 2 до 4 годин. Подібний розподіл спостерігається і щодо TikTok, де 41,7% користуються платформою понад 4 години на день, а 26,7% – у межах 2-4 годин. Це вказує на значну візуально-медійну орієнтованість цифрової поведінки державних службовців.

Ще однією надзвичайно поширеною платформою є Viber, який, ймовірно, виконує переважно функцію робочого та побутового спілкування: 42,5% респондентів використовують його понад 4 години на день, 31,3% – у межах 2-4 годин. Онлайн-месенджери WhatsApp, Telegram та Signal також мають високий рівень щоденного користування: 40,4% державних службовців вказали на понад 4 години активності, ще 25,2% – у межах 2-4 годин.

Facebook та Instagram займають проміжні позиції за інтенсивністю використання. У Facebook понад 4 години на день проводять 28,3% респондентів, 2-4 години – 27,1%. В Instagram понад 4 години перебувають 24,5% службовців, ще 22,0% – 2-4 години.

Натомість Twitter/X і Discord демонструють низьку частоту використання. Зокрема, 68,8% не користуються Twitter/X взагалі, а 80,1% – Discord. Це свідчить про обмежену популярність цих платформ серед державних службовців, можливо, через їхню орієнтацію на специфічні аудиторії або геймерське середовище (у випадку Discord).

Цікавою виявилася ситуація з Twitch, де спостерігається значна частка користувачів, які проводять у середньому 2-4 години на день (31,6%), попри те, що понад половина респондентів узагалі не користуються цією платформою (55,6%). Це може свідчити про сегментованість аудиторії та індивідуальну перевагу певних цифрових каналів залежно від професійних або особистих інтересів.

Таким чином, отримані дані свідчать про високу цифрову активність державних службовців, особливо в межах платформ, орієнтованих на відео- та текстову комунікацію, а також месенджерів (рис. 2.12).

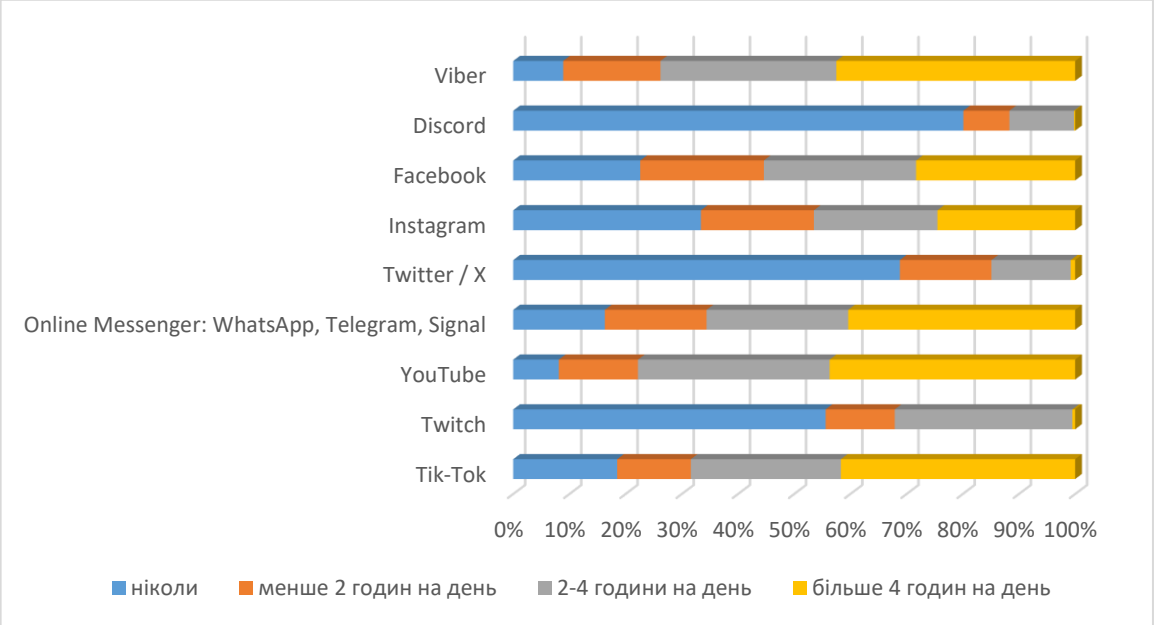

Рис. 2.12. Частота використання державними службовцями різних соціальних мереж (%).

Такий рівень присутності в соціальних мережах вимагає підвищеної уваги до питань цифрової етики, медіаграмотності, інформаційної безпеки та захисту персональних даних, що має бути інтегровано в систему державного управління й професійного навчання.

Також аналіз результатів щодо специфіки сприйняття та досвіду взаємодії респондентів із різними соціальними мережами та месенджерами виявив поширеність кіберхейту серед державних службовців (83% опитаних вважає, що за останній рік кількість кіберхейту збільшилася). Узагальнені результати поширеності кіберхейту на різних цифрових платформах представлені у табл. 2.6.

Таблиця 2.6

Найбільш поширені платформи кіберхейту (%).

	ніколи	***рідко***	***періодично***	***часто***	***не користуюся цією платформою***
Tik-Tok	14,1	16,9	22,3	28,5	18,2
Twitch	41,2	2,2	0,9	0,5	55,1
YouTube	17,6	31,3	29,5	13,1	8,5
Online Messenger: WhatsApp, Telegram, Signal	14,2	13,0	29,6	27,0	16,2
Twitter / X	13,2	8,8	5,8	3,8	68,4
Instagram	14,9	14,2	18,1	19,6	33,2
Facebook	33,5	17,6	13,9	12,1	22,9
Discord	16,8	1,6	0,7	0,4	80,5
Viber	14,3	29,3	29,6	18,2	8,6

Дані таблиці засвідчують, що найбільше проявів кіберхейту респонденти спостерігали на платформі TikTok: 28,5% опитаних зазначили, що часто стикаються з ненавистю на цій платформі, ще 22,3% – періодично, а 16,9% – рідко. Таким чином, майже 68% користувачів цієї платформи мали досвід взаємодії з контентом, що має риси кіберхейту, що вказує на особливу вразливість візуально-орієнтованого контенту до поширення ворожих наративів.

Суттєвий рівень поширення кіберхейту також зафіксовано в онлайн-месенджерах (WhatsApp, Telegram, Signal): 27% респондентів повідомили про

часті випадки ворожого контенту, 29,6% – про періодичні, ще 13% – про рідкісні. Це дозволяє говорити про ризики закритих або напіввідкритих цифрових комунікацій, де складніше здійснювати модерацію і контроль.

YouTube посідає третє місце за поширеністю кіберхейту: 13,1% респондентів вказали на часті випадки, 29,5% – на періодичні, а 31,3% – на рідкісні прояви. Таким чином, близько 74% користувачів цієї платформи принаймні епізодично зіштовхувалися з агресивним контентом.

На інших соціальних платформах частотність кіберхейту виявилась нижчою. Зокрема, в Instagram 19,6% респондентів вказали на часті прояви, 18,1% – на періодичні, 14,2% – на рідкісні. На Facebook ці показники становили відповідно 12,1%, 13,9% та 17,6%. Натомість значна частка опитаних узагалі не користуються цими платформами (33,2% – Instagram, 22,9% – Facebook), що частково зумовлює знижений рівень фіксації ворожого контенту.

У Viber 18,2% респондентів часто спостерігали кіберхейт, 29,6% – періодично, 29,3% – рідко, що вказує на потенційно високий рівень токсичності у групових чатах, з огляду на переважну побутову або робочу спрямованість комунікацій у цьому месенджері.

Найнижчі рівні агресивного контенту зафіксовано на Twitch і Discord, які відзначаються високим рівнем нефіксації (відповідно 55,1% і 80,5% респондентів не користуються цими платформами), а серед тих, хто все ж використовує їх, переважає повна відсутність досвіду зіткнення з кіберхейтом (41,2% – Twitch, 16,8% – Discord).

Таким чином, результати опитування свідчать про неоднорідність ризиків цифрової комунікації для державних службовців залежно від специфіки онлайн-платформ. Найбільші загрози виникають на візуально-орієнтованих соціальних мережах (TikTok, YouTube), а також у месенджерах, які дозволяють швидко поширювати інформацію у приватних чи групових чатах. Водночас традиційні платформи, як-от Facebook чи Instagram, демонструють нижчі рівні частоти кіберхейту серед опитаних (рис. 2.13).

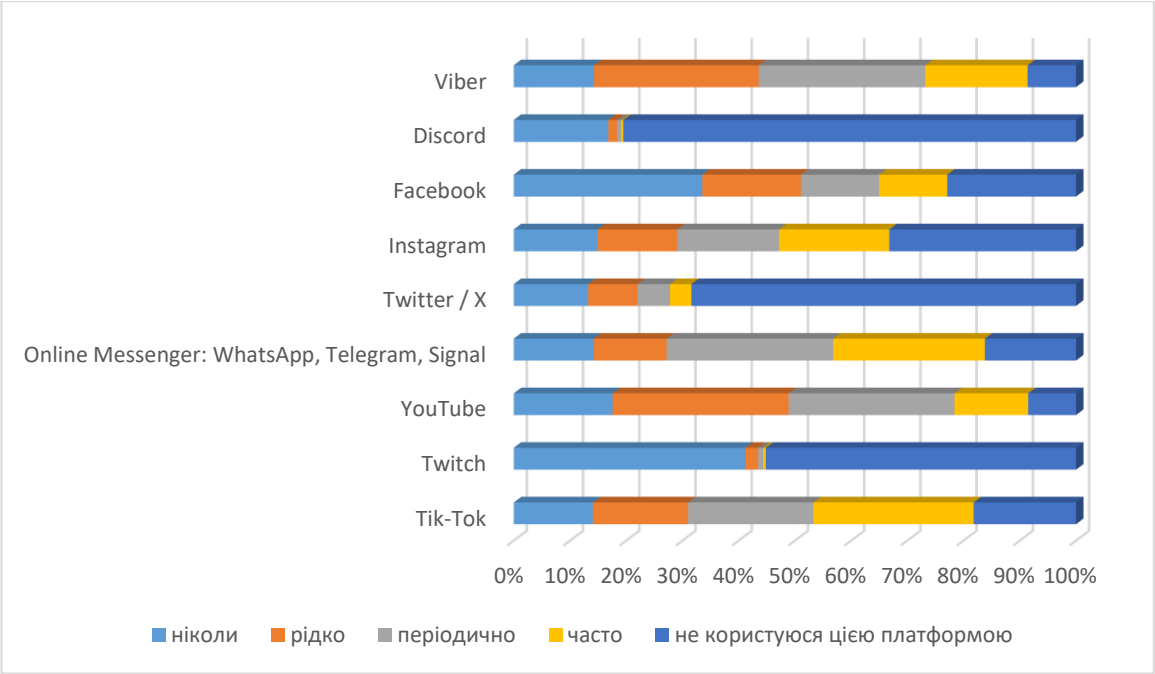

Рис. 2.13. Частота кіберхейту у різних соціальних мережах (%).

Ці дані дозволяють зробити висновок про необхідність диференційованого підходу до цифрової безпеки та формування культури взаємодії у різних цифрових середовищах.

Також аналіз результатів дозволив виявити найбільш поширені серед респондентів місця, де вони спостерігали прояви кіберхейту (табл. 2.7).

Таблиця 2.7

Найбільш поширені місця кіберхейту (%)

	ніколи	**рідко**	**періодично**	**часто**	**не знаю**
Образливі пости чи відеоролики у соціальних мережах чи інших інтернет-сайтах	8,7	23,4	28,6	23,5	15,8
Коментарі з образливим змістом у соціальних мережах, на веб-сайтах, форумах чи блогах	8,2	14,5	24,2	38,5	14,6
Групові чати (робочі, батьківські та ін.) (наприклад, у Viber, WhatsApp, Telegram та ін.)	22,7	30,6	18,4	11,6	16,7
Особисті повідомлення	30,4	30,6	14,1	9,4	15,5
Онлайн ігри	17,9	15,9	17,3	20,4	28,5

Отримані результати свідчать про те, що найчастіше кіберхейт фіксується у коментарях з образливим змістом у соціальних мережах, на веб-сайтах, форумах чи блогах. Так, 38,5% респондентів зазначили, що часто стикаються з подібними проявами, ще 24,2% – періодично, а 14,5% – рідко. Це означає, що саме коментарі залишаються найбільш агресивним сегментом цифрового простору, де домінує неконструктивна критика, приниження та мова ворожнечі.

Другою за поширеністю зоною кіберхейту є образливі пости чи відеоролики у соціальних мережах або на інших інтернет-сайтах. Часті випадки спостереження таких проявів відзначили 23,5% опитаних, періодичні – 28,6%, рідкісні – 23,4%. Це вказує на те, що публічний контент, який охоплює широку аудиторію, також часто слугує середовищем поширення ненависті.

На відміну від відкритих соціальних платформ, значно нижчі показники спостереження кіберхейту зафіксовано у групових чатах (наприклад, робочі або батьківські чати у Viber, WhatsApp, Telegram). Лише 11,6% респондентів стикаються з такими випадками часто, 18,4% – періодично, натомість 22,7% взагалі не стикалися з подібними ситуаціями. Ці дані демонструють, що приватні або напівприватні цифрові простори мають нижчий ризик поширення ненависті, хоча й не є повністю захищеними.

Ще менш поширеними місцями для кіберхейту виявилися особисті повідомлення, де лише 9,4% респондентів відзначили часті випадки отримання образливого контенту, 14,1% – періодичні, а 30,4% – взагалі не стикалися з таким явищем. Цей показник може свідчити як про більшу контрольованість особистих комунікацій, так і про специфіку професійної взаємодії державних службовців, яка зазвичай не передбачає агресії у приватному листуванні.

Онлайн-ігри залишаються середовищем, де респонденти фіксують прояви кіберхейту. Часті випадки зазначили 20,4%, ще 17,3% – періодично, 15,9% – рідко. Разом з тим, 28,5% респондентів не змогли визначитися з

відповіддю, що, ймовірно, вказує на низький рівень залученості державних службовців до онлайн-геймінгу або відсутність чіткої ідентифікації агресивного контенту в цьому середовищі.

У всіх п'яти категоріях залишається відчутна частка респондентів (від 14,6% до 28,5%), які не змогли визначитися з відповіддю («не знаю»), що може свідчити про неусвідомленість або нечутливість до проявів ненависті у цифровому просторі, а також про різний рівень цифрової компетентності серед державних службовців.

Таким чином, результати демонструють, що найвищий ризик зіткнення з кіберхейтом серед державних службовців існує у відкритих соціальних платформах, особливо у розділах коментарів та публічних постах. Приватні канали комунікації (чати та особисті повідомлення) мають значно нижчі показники, хоча й не є повністю захищеними від проявів онлайн-агресії. Водночас онлайн-ігри залишаються одним із менш контрольованих середовищ, що потребує уваги з боку дослідників та розробників політик цифрової безпеки (рис. 2.14).

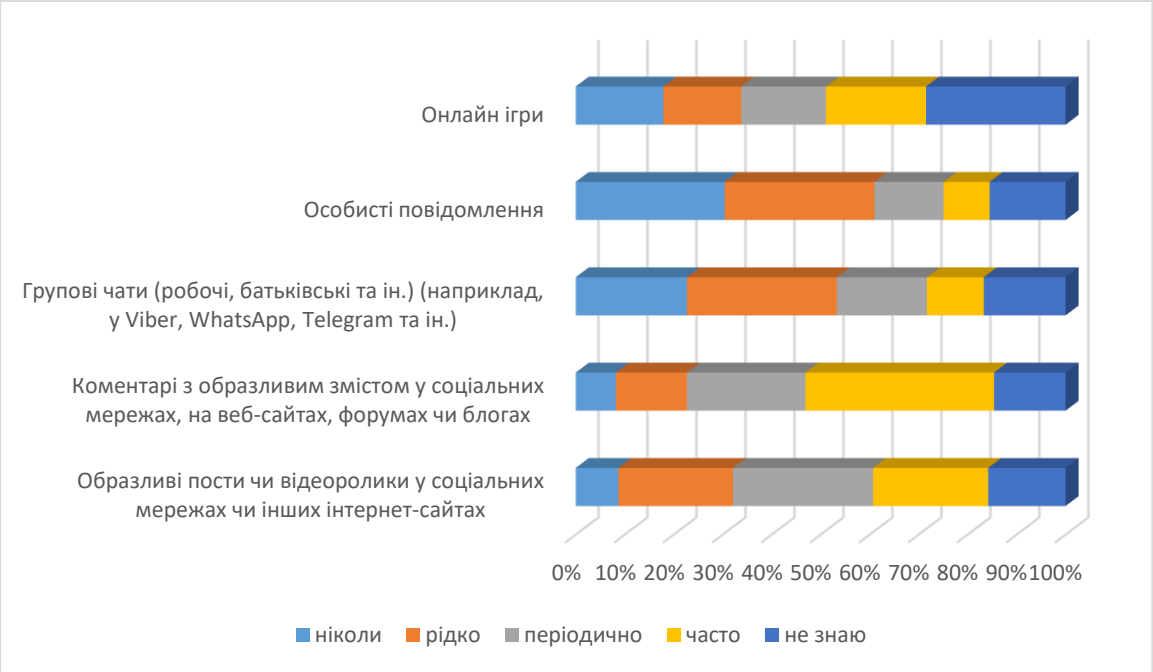

Рис. 2.14. Найпоширеніші місця кіберхейту (%).

Основними темами, навколо яких у цифровому середовищі найчастіше виникають прояви кіберхейту, виявилися питання, пов’язані з політикою (табл. 2.8).

Таблиця 2.8.

Розподіл респондентів за тематикою кіберхейту у соціальних мережах (%)

	ніколи	**кілька разів**	**принаймні щомісяця**	**частіше**	**не знаю**
Гомосексуальність чи сексуальність загалом. Це може включати думки або заяви про відносини між людьми, їх сексуальну орієнтацію або поведінку	23,4	25,5	12,8	18,9	19,4
Розмір людини (худа або повна статура)	14,7	27,4	14,7	27,6	16,6
Люди з іншим кольором шкіри	30,3	28,9	11,7	13,3	15,8
Люди з певними політичними поглядами	11,7	22,6	16,7	32,3	16,7
Тема політики/ політичні діячі	11,5	19,3	14,3	36,4	18,5
Люди з обмеженими можливостями здоров’я	39,4	29,2	6,4	6,7	18,3
Достаток людини (бідні чи багаті люди)	29,7	31,5	10,7	10,8	17,3
Люди інших культур та національностей	0,2	0,0	0,0	0,0	99,8
Біженці чи переселенці	27,7	26,7	10,0	14,1	21,5
Висловлювання та зміст, пов’язані з приналежністю до певної релігії	31,9	27,9	10,6	10,5	19,1
Вік	31,5	26,4	9,4	10,8	21,9
Жінки	43,5	25,4	7,3	6,3	17,5

Аналіз даних свідчить, що найчастіше прояви кіберхейту у соціальних мережах були пов’язані з темами політики та ідеології. Зокрема, 36,4% респондентів зазначили, що часто стикалися з образливими висловлюваннями щодо політичних діячів, а 32,3% – щодо осіб із певними політичними поглядами. Ще 14,3% і 16,7% відповідно зустрічали такі прояви принаймні щомісяця. Ці показники свідчать про високий рівень політичної конфліктності та поляризації в цифровому середовищі.

На другому місці за частотою згадувань кіберхейту опинилися теми, пов’язані із зовнішніми характеристиками особи, зокрема тілобудовою. 27,6% респондентів вказали, що часто спостерігали образливі висловлювання щодо худорлявості чи повноти, а ще 14,7% – щомісяця. Тема сексуальності також посідає помітне місце: 18,9% зазначили часту присутність подібного контенту, 12,8% – зустрічали його щомісяця.

Питання соціального статусу (достатку) стали предметом кіберхейту для 10,8% респондентів, які вказали, що часто стикалися з цим явищем, ще 10,7% – щомісяця. Також помірні показники зафіксовано щодо теми біженців та переселенців – 14,1% часто, 10,0% щомісяця, а також теми віку (10,8% і 9,4% відповідно) та релігії (10,5% і 10,6%).

Окрему увагу заслуговує тематика, пов’язана з кольором шкіри. Попри відносно нижчі значення, 13,3% респондентів вказали, що часто стикалися з расовими образами, а 11,7% – зустрічали їх щомісяця. Це свідчить про наявність расової дискримінації в онлайн-просторі, хоч і менш системної порівняно з політичним хейтом.

Натомість вкрай низький рівень спостереження кіберхейту виявлено стосовно теми етнічної чи культурної приналежності: 99,8% респондентів не змогли надати чіткої відповіді або не стикалися з такими проявами. Це може бути зумовлено як реальною відсутністю подібного контенту, так і низьким рівнем обізнаності або чутливості до цієї тематики серед державних службовців.

Найменш згадуваною темою кіберхейту стала дискримінація за ознакою статі (щодо жінок). Лише 6,3% респондентів зазначили, що часто спостерігали подібні прояви, 7,3% – щомісяця. Такі результати можуть свідчити про низьку помітність або замовчування проблеми гендерного хейту у професійному середовищі, а також про специфіку цифрової поведінки в державному управлінні.

Отже, результати дослідження засвідчують високу концентрацію агресивного цифрового контенту довкола політичної, тілесної та сексуальної

ідентичності, а також відносну нечутливість до деяких соціально значущих тем – етнічності, статі та інвалідності, що має бути враховано під час формування інформаційної безпеки в системі державного управління (рис. 2.15).

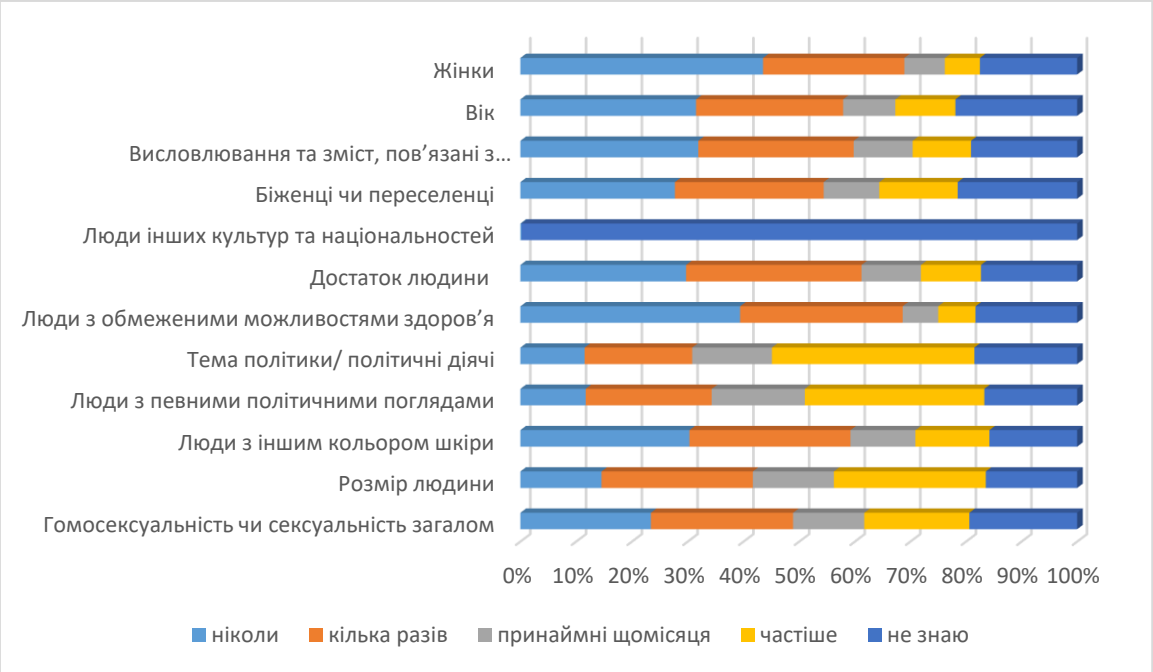

Рис. 2.15. Тематика кіберхейту у соціальних мережах (%).

Це підтверджує необхідність розробки цільових стратегій інформаційної безпеки та етичної поведінки у мережі, з особливим акцентом на попередження конфліктів та формування толерантності в цифровому середовищі.

Як видно з табл. 2.9, найпоширенішою формою негативного досвіду виявилося отримання злих чи образливих повідомлень, з якими стикалися 44,2% опитаних державних службовців хоча б один раз за останній рік (28,4% – рідко, 10,6% – періодично, 5,2% – часто). Це свідчить про поширеність вербальної агресії у цифрових комунікаціях, спрямованої безпосередньо на конкретну особу.

Менш поширеним, проте важливим з точки зору професійної репутації, виявилося явище поширення образливих повідомлень про респондента з метою публічного приниження або дискредитації. Лише 3,3% респондентів

стикалися з цим часто, 6,8% – періодично, тоді як більшість (79,1%) ніколи не зазнавала подібних випадків. Це дозволяє припустити, що пряма публічна дискредитація державних службовців через кіберпростір є менш масовою, ніж персоналізовані образи.

Таблиця 2.9

Найбільш поширені акти кіберхейту щодо державних службовців (%)

	ніколи	**рідко**	**періодично**	**часто**	**не знаю**
Мені надсилали злі чи образливі повідомлення	55,7	28,4	10,6	5,2	0,1
Про мене розсилали злі чи образливі повідомлення, щоб інші могли їх побачити	79,1	10,4	6,8	3,3	0,4
В Інтернеті мені погрожували, шантажували, чинили на мене тиск	81,6	10,2	4,5	3,1	0,6
Мені надходили повідомлення сексуального змісту, хоча я цього не хотів(ла)	75,1	12,1	7,7	4,3	0,8
Було опубліковано мої особисті чи ганебні фотографії	88,0	5,4	3,6	2,8	0,2

Серйозною, хоча менш поширеною формою кібернасильства стали погрози, шантаж або інші форми психологічного тиску в Інтернеті: 3,1% респондентів вказали, що часто стикалися з такими діями, ще 4,5% – періодично. Разом із тим, понад 80% учасників опитування не мали подібного негативного досвіду. Незважаючи на невисоку частотність, саме ці види агресії можуть мати найсерйозніші психологічні наслідки для особи та її професійної діяльності.

Окремої уваги заслуговують випадки отримання небажаних повідомлень сексуального характеру. З цим явищем стикалися 4,3% респондентів часто, 7,7% – періодично, що загалом становить майже чверть усіх опитаних. Це вказує на присутність сексуалізованих форм кібернасильства у відношенні до державних службовців, що потребує розробки окремих заходів реагування та підтримки постраждалих.

Найрідше фіксувалися випадки публікації особистих або компрометуючих фотографій. Лише 2,8% респондентів вказали, що часто стикалися з таким втручанням у приватність, тоді як абсолютна більшість (88%) не мали такого досвіду.

Загалом аналіз отриманих даних демонструє, що державні службовці піддаються різним формам кіберхейту з різною інтенсивністю та частотою (рис. 2.16). Найбільш поширеними є вербальні образи, у той час як більш тяжкі форми, такі як шантаж чи розповсюдження інтимної інформації, мають меншу, але все ж реальну присутність у цифровому середовищі. Це підтверджує необхідність вдосконалення політик кібербезпеки, розробки системи захисту та підтримки державних службовців, а також включення тем цифрової етики та психологічної стійкості до програм професійного навчання.

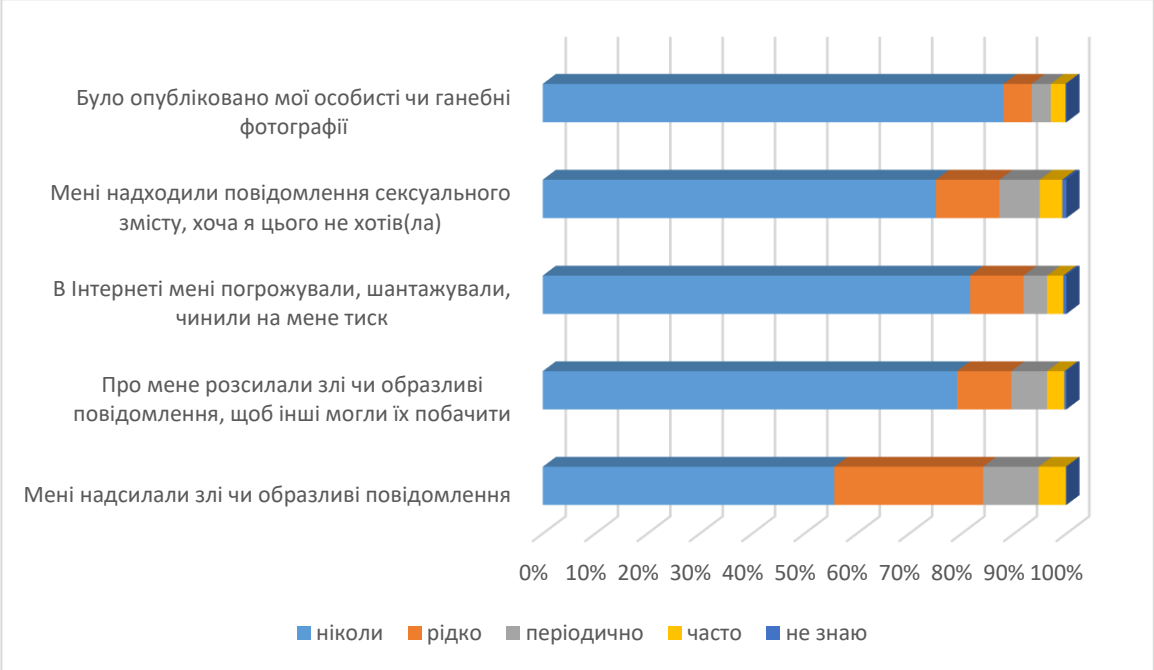

Рис. 2.16. Форми кіберхейту проти державних службовців (%.)

Найбільш поширеним простором для здійснення актів кіберхейту стали коментарі у соціальних мережах, на вебсайтах та в блогах (табл. 2.10). Зокрема, майже п’ята частина респондентів (19,3%) вказали, що часто стикаються з образливими висловлюваннями у коментарях, ще 16,6% зазначили, що це трапляється з ними іноді, а 18,4% – рідко. Таким чином,

майже половина опитаних мають той чи інший досвід зіткнення з ненавистю у коментарях, що підкреслює особливу вразливість відкритих дискусійних майданчиків.

Таблиця 2.10

Найпоширеніші місця актів кіберхейту щодо державних службовців (%)

	ніколи	**рідко**	**іноді**	**часто**	**не знаю**
у коментарях	45,6	18,4	16,6	19,3	0,1
у постах або на відео у соціальних мережах	52,8	18,4	14,8	13,8	0,2
у групових чатах	63,6	16,1	10,5	9,4	0,4
в особистих повідомленнях	61,1	18,6	10,7	9,3	0,3

Друге місце за поширеністю займають пости або відео у соціальних мережах, де 13,8% респондентів повідомили про часті випадки хейту, 14,8% – іноді, а 18,4% – рідко. Хоча рівень частої фіксації нижчий, ніж у коментарях, загальна залученість респондентів до подібних негативних ситуацій залишається високою.

Менш поширеним місцем фіксації кіберхейту є групові чати (наприклад, робочі або соціальні групи у месенджерах). Лише 9,4% опитаних вказали, що часто стикаються з образливими висловлюваннями у цьому форматі, ще 10,5% – іноді. Водночас, більшість респондентів (63,6%) не мали такого досвіду взагалі.

Найнижчий рівень частих проявів хейту зафіксовано у особистих повідомленнях: лише 9,3% респондентів стикалися з подібною поведінкою часто, 10,7% – іноді, а 61,1% не стикалися ніколи. Це може свідчити про те, що агресивна онлайн-поведінка щодо державних службовців частіше набуває публічних, ніж приватних форм.

Загалом отримані дані засвідчують, що найбільшу небезпеку для державних службовців становлять саме відкриті комунікаційні середовища, де висловлювання адресуються широкій аудиторії та можуть набувати форми масової онлайн-агресії (рис. 2.17). Водночас приватні канали комунікації, як-

от особисті повідомлення та групові чати, меншою мірою є простором для поширення хейту, хоча такі випадки все одно мають місце.

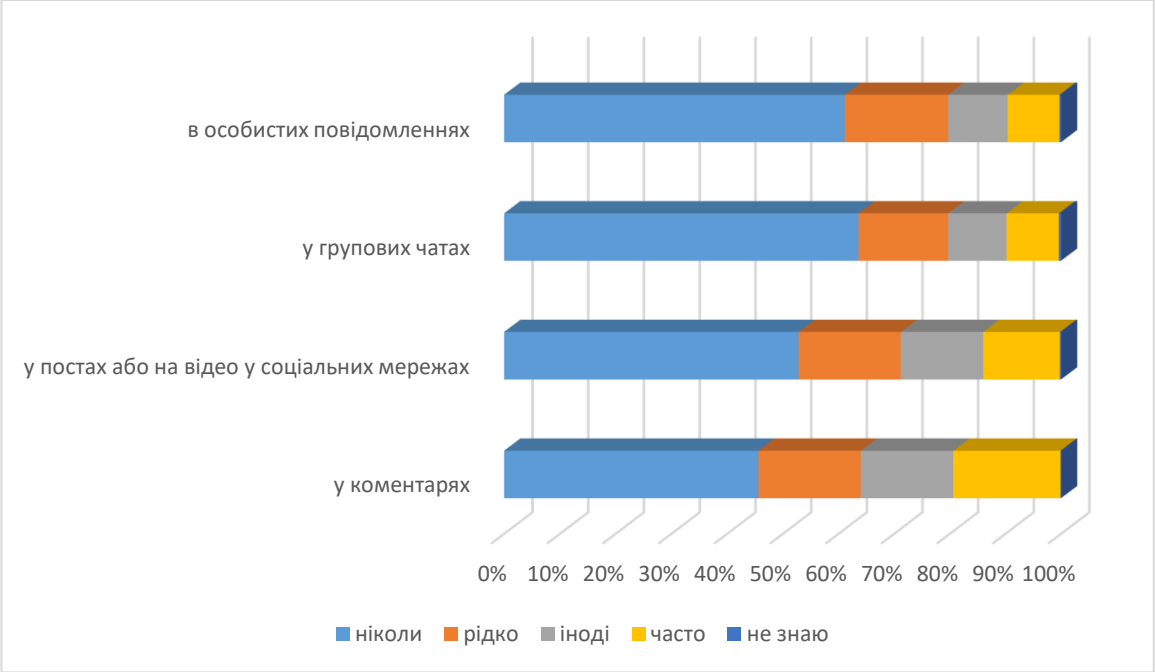

Рис. 2.17. Найпоширеніші місця актів кіберхейту щодо державних службовців (%).

Результати опитування вказують на потребу формування інформаційної культури та впровадження політик цифрової етики як на інституційному рівні, так і серед широкої громадськості, з метою зниження ризиків публічної дискредитації та психологічного тиску на працівників державної служби.

Дані, представлені у табл. 2.11, відображають поширеність спостереження державними службовцями випадків кіберхейту, спрямованого не безпосередньо проти них, а щодо осіб із їхнього соціального оточення: друзів, членів сім'ї, колег або керівництва. Такий підхід дозволяє оцінити ширший соціальний контекст онлайн-агресії, з якою опосередковано стикаються працівники державної служби.

Так, найбільш поширеним середовищем для фіксації актів ненависті щодо знайомих осіб стали коментарі у соціальних мережах, на вебсайтах або форумах. Зокрема, 8,0% респондентів зазначили, що часто стикалися з

подібними проявами, 15,2% – іноді, ще 17,4% – рідко. Водночас понад половина опитаних (59,1%) не мали такого досвіду взагалі.

Таблиця 2.11

Найпоширеніші місця актів хейту щодо друзів, членів сім'ї, колег або керівництва державних службовців(%)

	ніколи	***рідко***	***іноді***	***часто***	***не знаю***
у коментарях	59,1	17,4	15,2	8,0	0,3
у постах або на відео у соціальних мережах	58,9	21,4	12,6	6,6	0,5
у групових чатах	61,1	18,2	10,3	9,7	0,7
в особистих повідомленнях	61,5	21,6	9,1	7,4	0,4

Подібний розподіл спостерігається і щодо постів або відео у соціальних мережах, де 6,6% респондентів спостерігали хейт часто, 12,6% – іноді, а 21,4% – рідко. Це свідчить про те, що публічні форми онлайн-комунікації залишаються основними просторами для поширення образливих висловлювань не лише щодо самих державних службовців, але й щодо людей із їхнього близького кола.

У групових чатах акти хейту проти знайомих осіб фіксуються дещо рідше: 9,7% опитаних зазначили, що спостерігали подібне часто, 10,3% – іноді, ще 18,2% – рідко. Більшість респондентів (61,1%) не стикалися з такими випадками в чатах.

Найнижчі показники спостереження кіберхейту щодо знайомих осіб зафіксовано в середовищі особистих повідомлень. Лише 7,4% респондентів повідомили про часті випадки, 9,1% – про періодичні, а більшість (61,5%) не мали такого досвіду. Це підтверджує тенденцію, що персональні комунікації меншою мірою слугують простором для агресії проти третіх осіб.

Узагальнюючи отримані дані, можна констатувати, що державні службовці здебільшого стають свідками кіберхейту щодо своїх знайомих у публічних комунікаційних просторах соціальних мереж – у коментарях та публікаціях (рис. 2.18). При цьому закриті цифрові простори, такі як чати або приватні повідомлення, демонструють нижчий рівень подібних проявів.

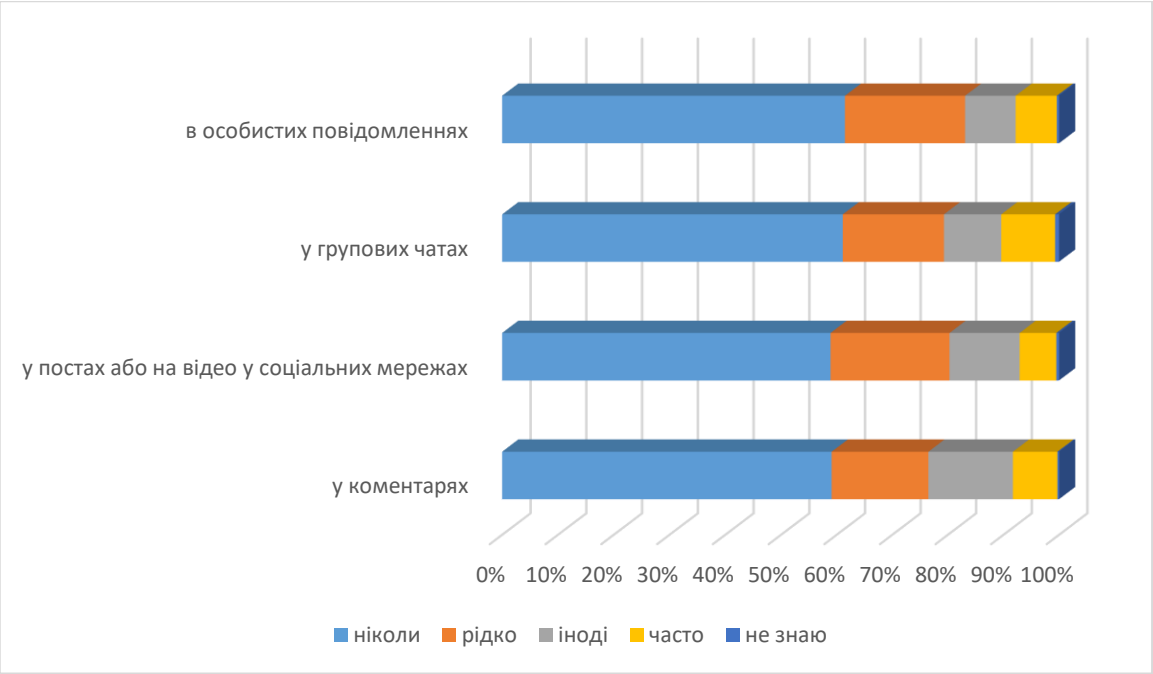

Рис. 2.18. Найпоширеніші місця актів кіберхейту щодо друзів, членів сім'ї, колег або керівництва державних службовців, %.

Ці результати підкреслюють важливість впровадження систем моніторингу, превентивних заходів та інформаційних кампаній, спрямованих не лише на захист самих державних службовців, але й на формування толерантного цифрового середовища для всієї спільноти.

Аналіз отриманих результатів також дає можливість виявити емоційне та когнітивне сприйняття державними службовцями проявів ненависті в Інтернеті, а також їхні внутрішні реакції на онлайн-агресію. Так, ми отримали широкий спектр ставлень – від активної протидії до байдужості чи навіть схвалення таких явищ (табл. 2.12.).

Найбільш поширеною реакцією респондентів є байдужість до проявів ненависті у цифровому просторі: 43,6% опитаних зазначили, що їм «все одно», ще 26,7% періодично демонструють подібне ставлення. Це вказує на певну нормалізацію або емоційну відстороненість значної частини державних службовців щодо онлайн-агресії.

Водночас 54,1% респондентів ніколи не відчували бажання протистояти проявам ненависті, лише 6,5% вказали, що часто мають таке прагнення, що

свідчить про низький рівень готовності до активної протидії хейту серед більшості опитаних. Це може бути пов'язано як із побоюванням негативних наслідків, так і з браком ефективних механізмів реагування.

Таблиця 2.12

Загальне сприйняття державними службовцями ненависті в Інтернеті (%)

	ніколи	***рідко***	***періодично***	***часто***	***не знаю***
У мене з'являється бажання протистояти цьому	54,1	24,9	14,3	6,5	0,2
Я почуваюся безпорадним	45,2	39,3	9,7	5,3	0,5
Мені все одно	18,1	11,3	26,7	43,6	0,3
Мені подобається спостерігати за цим/ мені смішно бачити ненависть в Інтернеті	58,4	23,3	12,7	5,5	0,1
Я намагаюся забути про це	26,1	24,0	28,2	21,3	0,4
Я злюсь через це	19,9	39,1	27,5	13,4	0,1
Я засмучуюсь через це	48,2	25,3	14,8	11,5	0,2
Я відчуваю, що моя думка збігається з цими висловлюваннями	16,3	17,2	26,7	39,7	0,1
Мене це розважає	59,8	26,7	8,2	4,9	0,4
З'являється бажання помститися цій людині	76,8	13,4	6,7	2,9	0,2

Значна частка респондентів демонструє почуття безпорадності у ситуаціях, пов'язаних з онлайн-агресією: 5,3% відчувають це часто, ще 9,7% – періодично, тоді як 45,2% не мали таких відчуттів взагалі. Це вказує на амбівалентність сприйняття: поруч із байдужістю існує значний прошарок осіб, які переживають тривогу та розгубленість.

Цікавими є дані щодо емоційної напруги та роздратування: 13,4% респондентів часто зляться через побачене, ще 27,5% – періодично, а 39,1% – рідко. Аналогічно, засмученість фіксується як частою реакцією у 11,5% респондентів та періодичною – у 14,8%.

Водночас невелика, але помітна частка державних службовців продемонструвала позитивне або нейтрально-гумористичне ставлення до

онлайн-ненависті. Так, 5,5% зазначили, що їм смішно бачити прояви хейту, а ще 4,9% повідомили, що такі ситуації їх розважають. Це може свідчити про девальвацію серйозності подібних явищ у частини респондентів.

Увагу привертає також ставлення респондентів до змісту агресивних висловлювань: 39,7% опитаних часто відчували, що їхня думка збігається з побаченими хейтерами судженнями, ще 26,7% іноді погоджувалися з такими висловлюваннями. Це підкреслює ризик поширення та прийняття деструктивних наративів навіть серед професійної аудиторії.

Водночас показник бажання помститися є найнижчим: лише 2,9% респондентів часто відчували таке бажання, тоді як абсолютна більшість (76,8%) взагалі не схильні до такого типу реакції. Це свідчить про досить високий рівень самоконтролю та соціальної стриманості серед державних службовців.

Загалом результати демонструють складну палітру емоційних та поведінкових реакцій державних службовців на онлайн-ненависть: від байдужості й уникання до емоційної залученості та часткового прийняття агресивних висловлювань (рис. 2.19).

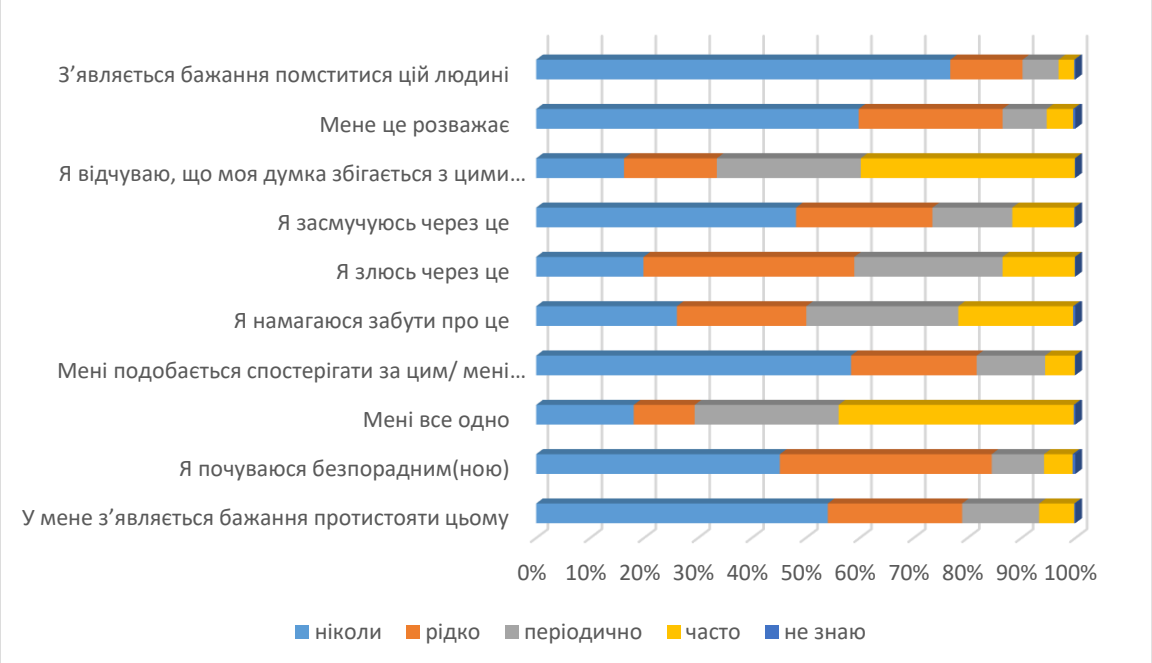

Рис. 2.19. Загальне сприйняття державними службовцями ненависті в Інтернеті, %.

Це підкреслює актуальність розробки стратегій психологічної підтримки, інформаційної просвіти та формування навичок критичного сприйняття онлайн-контенту у системі державного управління.

Щодо емоційних реакцій державних службовців на випадки кіберхейту, спрямованих проти них особисто, або проти людей з їхнього найближчого соціального оточення – друзів, родичів, колег або керівництва, отримані результати дозволяють простежити як емпатійні прояви, так і емоційну дистанційованість щодо таких ситуацій (табл. 2.13).

Таблиця 2.13

Реакції державних службовців на кіберхейт, спрямований проти них та людей з їхнього особистого оточення (%)

	ніколи	***рідко***	***періодично***	***часто***	***не знаю***
У мене з'являється бажання протистояти цьому	18,3	21,2	20,1	40,3	0,1
Я почуваюся безпорадним	32,6	28,9	20,2	17,9	0,4
Мені все одно	64,8	13,7	12,5	8,7	0,3
Мені подобається спостерігати за цим/ мені смішно бачити ненависть в Інтернеті	69,1	22,0	5,9	2,4	0,6
Я намагаюся забути про це	46,0	33,2	14,7	5,6	0,5
Я злюсь через це	8,1	10,1	32,2	49,5	0,1
Я засмучуюсь через це	10,6	14,8	25,9	48,4	0,3
Я відчуваю, що моя думка збігається з цими висловлюваннями	56,3	17,2	16,7	9,7	0,1
З'являється бажання помститися цій людині	12,1	19,2	27,4	41,2	0,1

Найпоширенішою реакцією є бажання протистояти агресії: 40,3% респондентів відзначили, що часто відчувають потребу діяти у відповідь на випадки онлайн-ненависті, ще 20,1% відчувають це періодично, а 21,2% – рідко. Лише 18,3% учасників опитування ніколи не переживали подібного емоційного стану. Це свідчить про достатньо високий рівень громадянської

залученості та готовність до активної протидії агресії у цифровому середовищі.

Водночас емоційна безпорадність проявляється менш виражено: 17,9% респондентів часто відчували себе безпорадними, 20,2% – періодично, тоді як 32,6% взагалі не переживали подібного стану. Це вказує на те, що хоча частина державних службовців все ж відчуває розгубленість і неспроможність діяти, для більшості такі ситуації не є причиною втрати контролю або рішучості в діях або реакціях.

Найбільша емоційна дистанційованість фіксується у респондентів, які вказали, що їм все одно у випадках проявів кіберхейту. Таку позицію займає 64,8% опитаних (ніколи не відчували емоційної залученості), лише 8,7% часто проявляли байдужість. Це може бути пов’язано як із професійною стійкістю, так і з емоційним виснаженням або адаптацією до високої кількості подібних проявів у цифровій реальності.

Позитивне або гумористичне сприйняття кіберхейту фіксується рідко: лише 2,4% респондентів зазначили, що часто отримують задоволення або сміються з подібних проявів, ще 5,9% – періодично. Переважна більшість (69,1%) взагалі не поділяє подібного ставлення.

Цікавою є поширеність стратегії уникнення, коли людина намагається забути про побачене: 5,6% респондентів зазначили, що часто вдаються до такої тактики, 14,7% – іноді, а найбільша частка – 46,0% – взагалі не використовують таку стратегію. Це свідчить про досить помірний рівень психологічного захисту через витіснення негативного досвіду.

Водночас показники злості (49,5% – часто, 32,2% – періодично) та засмученості (48,4% – часто, 25,9% – періодично) демонструють високий рівень емоційної залученості державних службовців до ситуацій онлайн-агресії. Це свідчить про те, що навіть за умов професійної дистанції значна частина респондентів не залишається емоційно байдужою до проявів хейту.

Більшість респондентів відкидають ідентифікацію із агресорами: 56,3% ніколи не поділяли висловлювань, які містять прояви ненависті, тоді як лише

9,7% часто погоджувалися з подібними судженнями. Це підтверджує домінування у вибірці ціннісних орієнтацій, несумісних із толеруванням агресії у цифровому просторі.

Звертає на себе увагу рівень потреби у помсті: 41,2% респондентів відчувають таку емоцію часто, ще 27,4% – періодично. Це одна з найпоширеніших реакцій серед опитаних, що може слугувати індикатором внутрішнього конфлікту між емоційним переживанням несправедливості та усвідомленням професійної необхідності зберігати стриманість.

Таким чином, емоційні реакції державних службовців на кіберхейт відзначаються переважанням негативних емоцій – злості, засмученості, бажання протистояти – поряд із менш вираженими проявами безпорадності та байдужості (рис. 2.20).

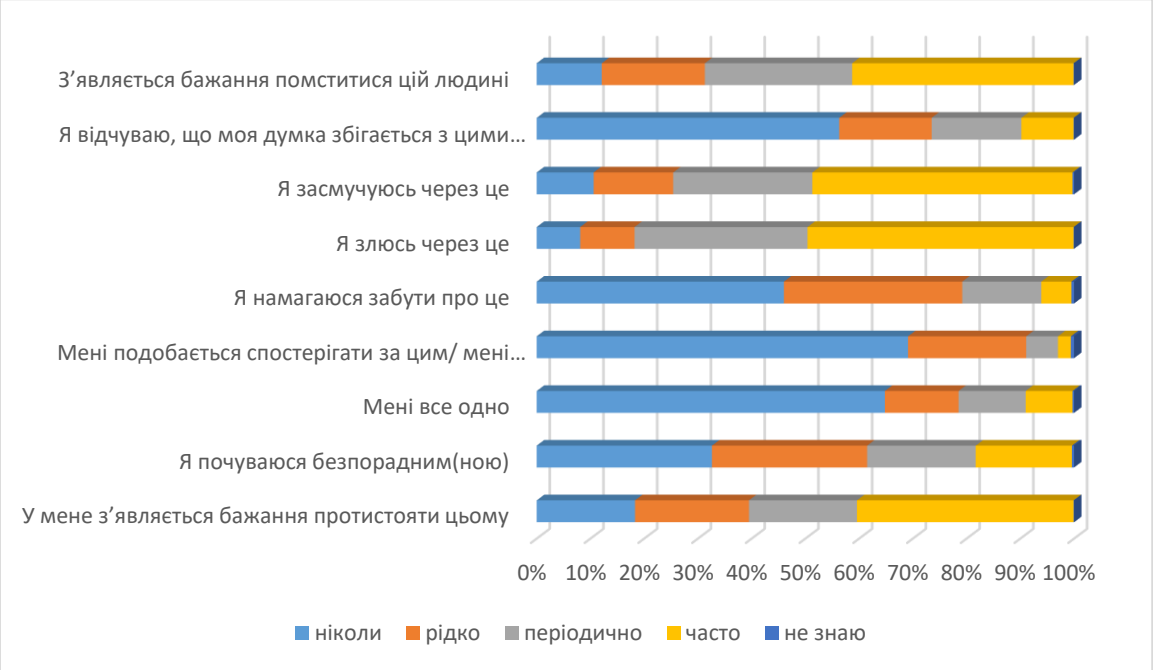

Рис. 2.20. Реакції державних службовців на кіберхейт, спрямований проти них та людей з їхнього особистого оточення, %.

Ці результати підкреслюють важливість розвитку інституційної підтримки не лише для безпосередніх жертв онлайн-агресії, але й для тих, хто опосередковано залучений у такі ситуації як свідок чи учасник соціальної групи. Це засвідчує наявність як високого рівня емпатійності, так і

внутрішньої психологічної напруги, що потребує врахування при розробці програм підтримки та запобігання емоційному вигоранню в умовах цифрової взаємодії.

Аналіз відповідей державних службовців на питання анкети щодо способів реагування на випадки кіберхейту дозволяє виокремити основні поведінкові стратегії, що застосовуються у цифровому середовищі, та охарактеризувати рівень готовності респондентів до конструктивної або захисної поведінки в умовах онлайн-агресії (табл. 2.14).

Табл.2.14

Стратегії поведінки державних службовців щодо кіберхейту загалом (%)

	абсолютно не згоден	***не згоден***	***важко відповісти***	***згоден***	***повністю згоден***
Ніяк, не реагую	36,4	34,6	3,5	13,4	12,1
Я закриваю сайт або програму	21,5	23,6	3,4	30,3	21,2
На деякий час я перестаю користуватися Інтернетом	10,8	14,2	2,1	36,6	36,3
Я обговорюю це зі своїми друзями	13,2	35,2	5,4	25,2	21,0
Я розповідаю про це своїм колегам	12,7	33,4	4,1	26,4	23,4
Я відповідаю і вступаю в конфронтацію з людиною	14,3	23,4	2,1	31,3	28,9
Я говорю про це зі своїм керівником	21,9	46,8	1,2	13,1	17
Я повідомляю про цей випадок у поліцію	20,5	49,6	1,7	15,1	13,1
Я коригую/міняю свої налаштування конфіденційності	28,8	50,1	4,8	11,1	5,2
Я повідомляю платформу про те, що певний контент або облікові записи, про які я знаю, можуть бути токсичними, щоб його можна було видалити чи заблокувати	26,6	48,3	7,9	10,1	7,1
Я використовую функції блокування та сповіщення, коли стикаюся з ненавистю в Інтернеті	27,9	48,9	6,3	10,5	6,4

Найпоширенішою реакцією державних службовців на прояви кіберхейту є пасивне ігнорування, що підтверджується високими показниками за твердженням «Ніяк, не реагую»: загалом 71,0% опитаних (36,4% — абсолютно не згоден і 34,6% — не згоден) не погоджуються з тим, що залишають подібні ситуації без реакції, натомість лише 12,1% повністю згодні з такою поведінкою. Це свідчить про суперечливість у ставленні до тактики ігнорування та небажання для більшості респондентів залишатися осторонь.

Досить поширеною є стратегія короткострокового уникнення, яка реалізується через закриття вебсайтів чи програм (30,3% згодні, 21,2% повністю згодні) або тимчасове припинення використання Інтернету (36,6% згодні, 36,3% повністю згодні). Ці показники вказують на прагнення значної частини державних службовців мінімізувати вплив негативного контенту шляхом дистанціювання від цифрового простору.

Помірно поширеними є стратегії соціальної підтримки: 46,2% респондентів (25,2% згодні, 21,0% повністю згодні) зазначили, що обговорюють такі ситуації з друзями, а 49,8% (26,4% згодні, 23,4% повністю згодні) — з колегами. Це свідчить про важливість соціального оточення для емоційного розвантаження та пошуку підтримки у професійному чи особистому середовищі.

Досить високий рівень отримала стратегія активної конфронтації, коли респонденти вступають у дискусію або відповідають агресору: 31,3% згодні з цією тактикою, ще 28,9% — повністю згодні. Це вказує на те, що майже 60% опитаних готові відкрито реагувати на прояви кіберхейту, що потенційно може призводити до ескалації конфліктів, але також свідчить про відчуття особистої відповідальності за цифрову комунікацію.

Водночас звернення до формальних механізмів реагування є менш поширеним: лише 30,1% респондентів (13,1% — повністю згодні, 15,1% — згодні) повідомляють про випадки кіберхейту до поліції, і лише 30,1% (13,1% + 17,0%) обговорюють це з керівництвом. Це демонструє недостатній рівень

довіри або низьку ефективність інституційних каналів реагування в очах респондентів.

Ще менш активними є технічні стратегії безпеки, такі як зміна налаштувань конфіденційності (16,3% загалом згодні) чи використання функцій блокування (16,9% згодні/повністю згодні). Повідомлення платформи про порушення також застосовується порівняно рідко: лише 17,2% респондентів вказали, що схвалюють цю дію. Це може свідчити про низький рівень цифрової грамотності або недовіру до ефективності платформних механізмів захисту.

Узагальнені результати демонструють, що поведінка державних службовців у ситуаціях кіберхейту є переважно реактивною та ситуативною (рис. 2.21). Домінують стратегії уникнення або пошуку підтримки в соціальному колі, тоді як формальні інституційні та технічні методи залишаються малозадіяними.

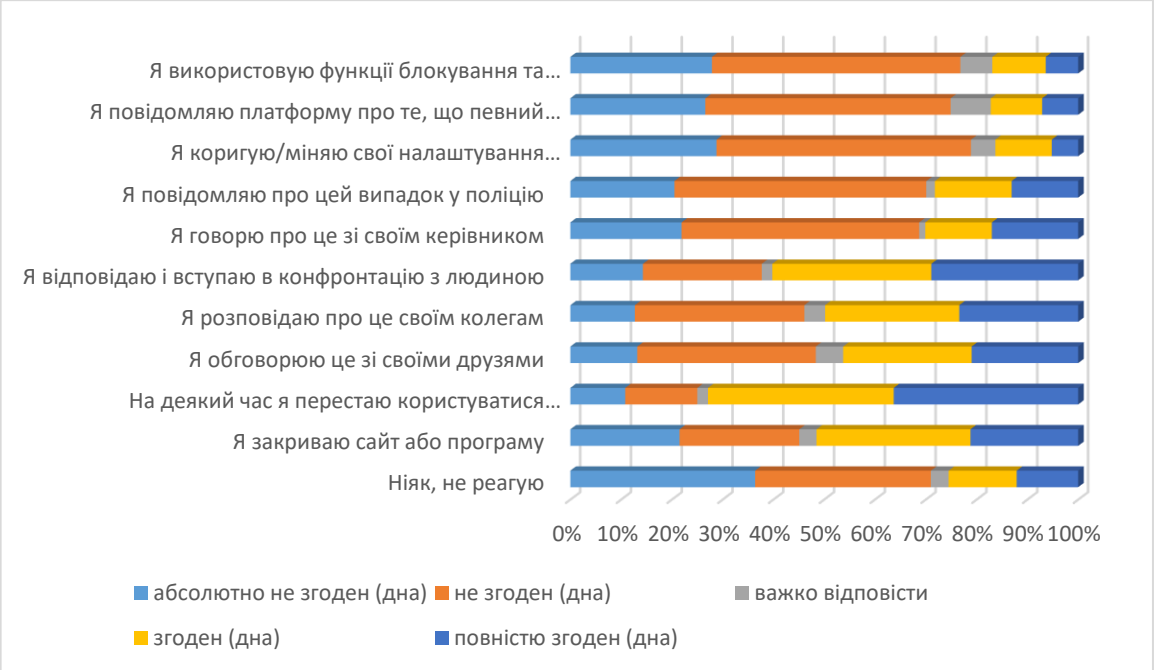

Рис. 2.21. Стратегії поведінки державних службовців щодо кіберхейту загалом (%).

Це вказує на необхідність підвищення рівня цифрової обізнаності державних службовців, формування навичок безпечної поведінки в

кіберпросторі та розвитку механізмів офіційної підтримки в умовах інформаційних загроз.

Щодо проявів кіберхейту, спрямованих безпосередньо проти державних службовців або проти осіб з їхнього особистого соціального оточення, отримані дані вказують на те, що респонденти демонструють більш активні та емоційно забарвлені стратегії поведінки порівняно з абстрактним сприйняттям кіберхейту в Інтернеті загалом (табл. 2.15).

Таблиця 2.15

Стратегії поведінки державних службовців щодо кіберхейту, спрямованого проти самих державних службовців та їхнього оточення (%)

	абсолютно не згоден	***не згоден***	***важко відповісти***	***згоден***	***повністю згоден***
Ніяк, не реагую	34,4	56,6	1,5	4,4	3,1
Я говорю на цю тему з друзями	11,2	15,2	1,3	49,2	23,1
Я говорю на цю тему з колегами	22,7	44,4	3,1	16,4	13,4
Я відповідаю і вступаю у конфронтацію з людиною	4,3	13,4	2,1	41,3	38,9
Я говорю на цю тему з керівництвом	31,9	56,2	1,2	7,6	3,1
Я повідомляю про цей випадок у поліцію	20,4	39,5	0,1	26,2	13,8
Я коригую свої налаштування конфіденційності	29,7	52,1	3,7	9,1	5,4
Я повідомляю платформу про те, що певний контент або облікові записи, про які я знаю, можуть бути токсичними, щоб його можна було видалити чи заблокувати	7,3	8,6	3,9	46,1	34,1
Я використовую функції блокування та сповіщення, коли стикаюся з ненавистю в Інтернеті	7,6	18,9	6,3	40,9	26,3

Найменш прийнятною для більшості державних службовців є стратегія пасивного ігнорування: 56,6% опитаних не погоджуються з тим, що не реагують на такі ситуації, ще 34,4% категорично не згодні з такою поведінкою. Лише 7,5% респондентів (4,4% згодні, 3,1% повністю згодні) схиляються до

повного ігнорування. Це свідчить про загальну неприйнятність байдужості у випадках особистого або соціального залучення до ситуацій кіберагресії.

Натомість переважають стратегії соціальної підтримки, зокрема обговорення ситуації з друзями (49,2% згодні, 23,1% повністю згодні, що загалом становить понад 72% схвалення цієї поведінки). Обговорення таких випадків з колегами є менш поширеним: 29,8% респондентів демонструють згоду або повну згоду з цим варіантом, тоді як більшість (67,1%) не схвалюють такої поведінки. Це підкреслює значущість неформальної підтримки та, водночас, низький рівень інституційної відкритості щодо таких тем у професійному середовищі.

Досить високий рівень демонструє активна стратегія конфронтації: 41,3% респондентів згодні, а ще 38,9% повністю згодні з тим, що відповідають агресору та вступають у конфлікт. Сукупно це становить майже 80%, що свідчить про значну готовність до відкритого протистояння проявам ненависті, якщо вони стосуються особисто службовця чи його оточення.

Водночас звернення до формальних механізмів реагування, таких як обговорення з керівництвом (10,7% згодні або повністю згодні) або повідомлення поліції (40% схвалення), залишається менш поширеним. Переважна більшість респондентів не схильна звертатися до офіційних структур, що може свідчити про брак довіри або низьку ефективність подібних дій у сприйнятті державних службовців.

Щодо технічних стратегій безпеки, то їх використання демонструє помірні показники. Так, зміна налаштувань конфіденційності отримала лише 14,5% позитивних відповідей, використання функцій блокування та сповіщень — 67,2% схвалення (40,9% згодні, 26,3% повністю згодні), а звернення до адміністрації платформи – 80,2% позитивних відповідей. Ці результати вказують на поступове зростання усвідомленості щодо цифрових інструментів захисту, однак рівень їх використання залишається нерівномірним.

Узагальнено, можна стверджувати, що державні службовці у випадках персональної загрози з боку кіберхейту демонструють переважно активні

стратегії реагування: через соціальну підтримку, відкриту конфронтацію або часткове використання технічних засобів захисту. Водночас звернення до інституційних структур та офіційних процедур залишається менш поширеним (рис. 2.22).

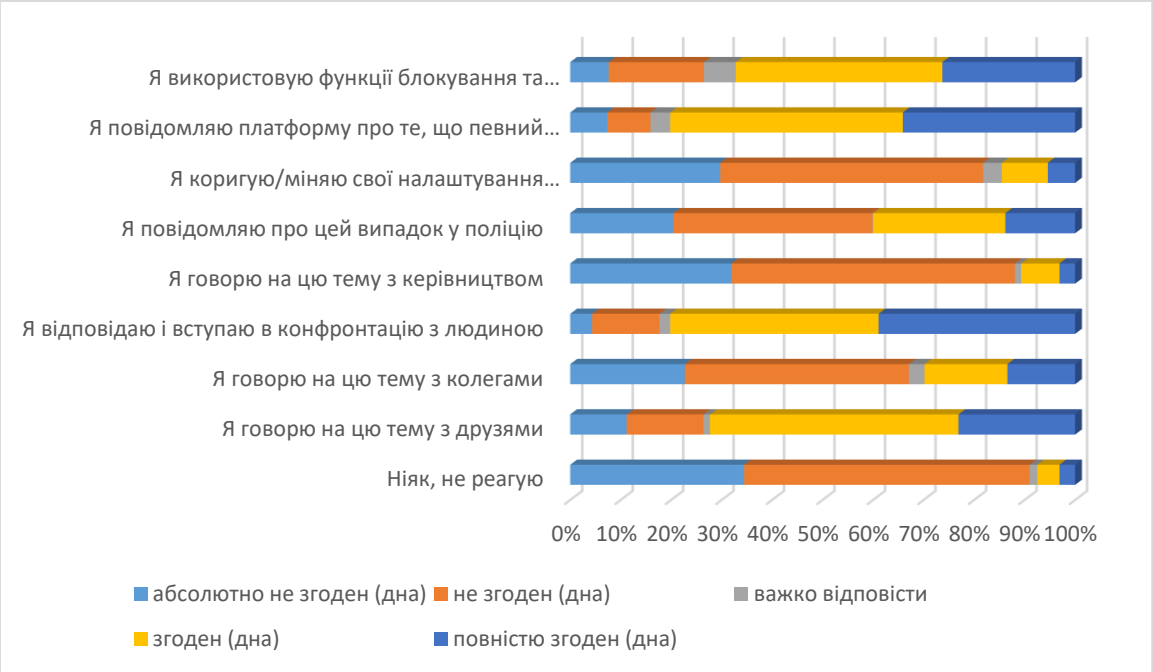

Рис. 2.22. Стратегії поведінки державних службовців щодо кіберхейту, спрямованого проти самих державних службовців та їхнього оточення (%).

Ці результати засвідчують необхідність підвищення рівня цифрової обізнаності державних службовців, розвитку механізмів внутрішньої підтримки у професійному середовищі та формування культури нульової толерантності до проявів онлайн-агресії.

Аналіз результатів опитування, спрямованого на виявлення ролі державних службовців як потенційних джерел агресивних висловлювань у цифровому середовищі, засвідчив, що понад 23,9% респондентів визнали, що часто поширювали або висловлювали в Інтернеті думки чи коментарі, які могли бути образливими для інших осіб (рис. 2.23). Йдеться про повідомлення грубого, особистісного чи залякуючого характеру, а також висловлювання, спрямовані проти людей за ознаками національності, етнічного походження, релігії, статі, гендерної ідентичності чи сексуальної орієнтації.

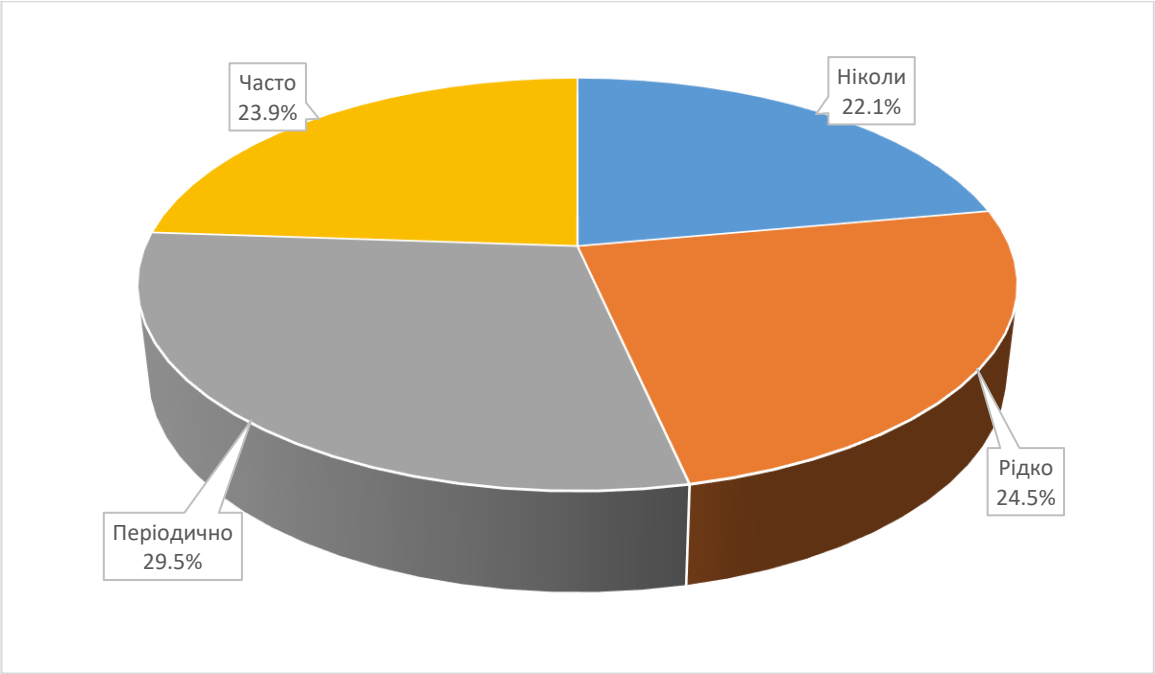

Рис. 2.23. Ролі державних службовців як потенційних агресорів у цифровому середовищі (%).

Ще 29,5% опитаних зазначили, що подібна поведінка траплялася з їхнього боку періодично, 24,5% – рідко, тоді як лише 22,1% респондентів повідомили, що ніколи не здійснювали подібних дій у цифровому середовищі.

Отримані дані свідчать про те, що певна частка державних службовців не лише виступає жертвами кіберхейту, але й сама може бути залученою до відтворення агресивних практик в Інтернеті. Це підкреслює актуальність формування високих етичних стандартів поведінки у цифровому просторі, а також розвитку цифрової культури, заснованої на принципах толерантності, недискримінації та відповідальності за контент онлайн-комунікацій.

Аналіз отриманих даних також дозволяє виокремити основні мотиви, що зумовлюють агресивну поведінку державних службовців у цифровому просторі. Дослідження демонструє, що причини проявів агресії є багатофакторними, охоплюють як ситуативні емоційні стани, так і міжособистісні конфлікти та соціальні настанови (табл. 2.16).

Однією з найпоширеніших причин участі в агресивних діях у мережі респонденти назвали особистий конфлікт з конкретною особою: 48,3%

державних службовців погодилися з цим твердженням, ще 31,2% — повністю погодилися. Таким чином, майже 80% респондентів визнають, що власні негативні взаємини можуть стати підґрунтям для агресивної поведінки в Інтернеті.

Таблиця 2.16

Причини агресії з боку державних службовців у кіберпросторі (%)

	абсолютно не згоден	***не згоден***	***важко відповісти***	***згоден***	***повністю згоден***
Тому що ця людина заслужила на це	18,8	24,7	3,2	31,1	22,2
Тому що у мене неприємності з цією людиною	9,2	10,2	1,1	48,3	31,2
Тому що ця людина також сказала або поділилася чимось неприємним щодо мене	13,8	19,7	1,2	42,1	23,2
Просто заради забави / думаю це смішно	31,7	39,6	3,2	15,3	10,2
Щоб помститися за інших, яких образили	19,6	25,7	1,3	31,2	22,2
Тому що мені нудно	42,6	41,6	1,2	8,3	6,3
Тому що в мене був поганий настрій	5,6	9,4	1,1	47,2	36,7
Тому що інші теж так роблять	40,1	39,9	2,7	9,1	8,2
Тому що це круто	37,7	38,5	4,8	9,3	9,7
Тому що я хочу висловити свою думку	10,0	12,1	1,3	46,8	29,8

Високі показники також продемонструвало твердження про реакцію у відповідь на попередні образи з боку іншої особи: 42,1% респондентів згодні з цим, а ще 23,2% повністю згодні, що свідчить про тенденцію до «дзеркальної» агресії як механізму самозахисту чи відплати.

Порівняно значущим чинником є і переконання, що людина «заслуговує» на агресивне ставлення: понад половина опитаних (31,1% згодні, 22,2% повністю згодні) підтримали цю думку, що вказує на схильність до раціоналізації власних агресивних дій у відповідності до поведінки інших.

Менш поширеною, але все ж вагомою причиною є бажання помсти за третіх осіб, яких образили: понад половина респондентів (31,2% згодні, 22,2%

повністю згодні) вважають виправданою агресію у таких випадках. Це може свідчити про наявність колективістських настанов або відчуття соціальної справедливості.

Одним з важливих висновків аналізу є те, що емоційний стан особи є суттєвим фактором агресивної поведінки: 47,2% респондентів згодні, а 36,7% повністю згодні, що поганий настрій ставав причиною їхніх образливих висловлювань в Інтернеті. Це дозволяє розглядати прояви кіберхейту не лише як раціональні реакції, а й як імпульсивні вчинки, зумовлені психоемоційною напругою.

Натомість такі фактори як нудьга (8,3% згодні, 6,3% повністю згодні), бажання бути «крутим» (9,3% згодні, 9,7% повністю згодні) або наслідування поведінки інших (9,1% згодні, 8,2% повністю згодні) мають низький рівень схвалення серед респондентів. Більшість опитаних категорично не погоджуються з такими поясненнями власної агресії, що свідчить про відсутність схильності до агресії «заради розваги» чи через конформізм.

Значна частина державних службовців виправдовують агресивну поведінку у випадках, коли вона є способом висловлення власної думки: майже 76,6% опитаних (46,8% згодні, 29,8% повністю згодні) підтримують таку позицію. Це вказує на тонку межу між свободою вираження поглядів і потенційною агресією у цифровій комунікації.

Узагальнюючи результати, можна зробити висновок, що найбільш значущими мотивами агресивної поведінки державних службовців у кіберпросторі є особисті конфлікти, реакція на образу, емоційні стани та потреба самовираження (рис. 2.24). Водночас малозначущими є соціальні або ситуативно-розважальні фактори.

Ці результати підкреслюють важливість розвитку навичок емоційного саморегулювання, цифрової етики та підвищення правової культури державних службовців у контексті їхньої професійної поведінки в кіберпросторі.

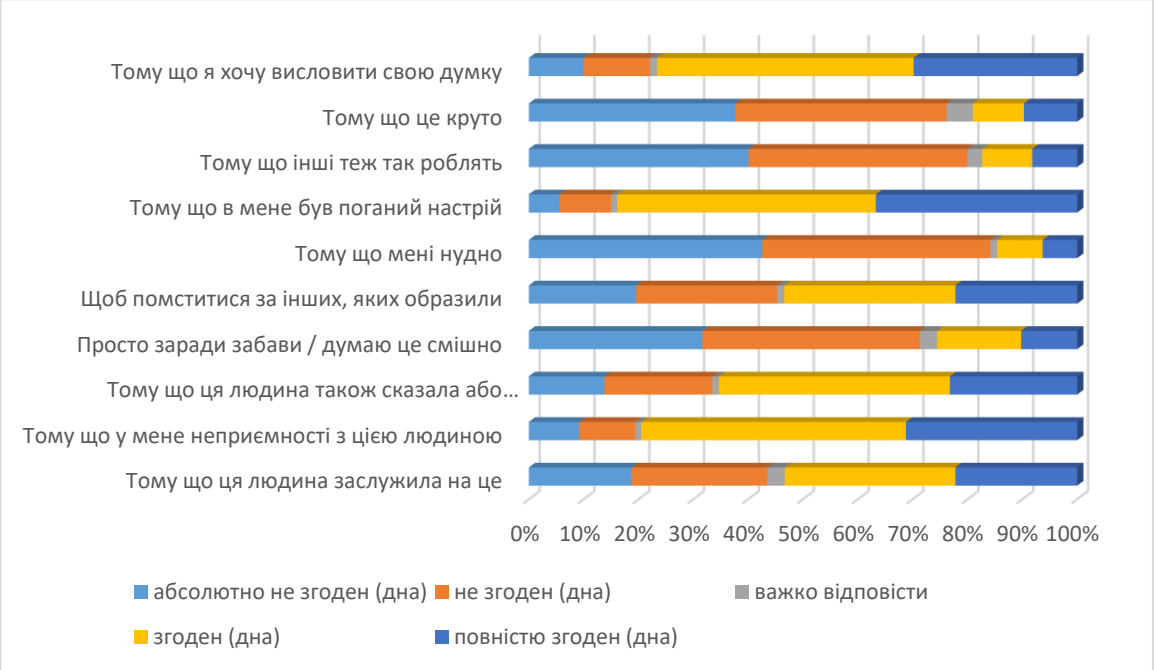

Рис. 2.24. Мотиви агресивної поведінки державних службовців у кіберпросторі (%).

Аналіз відповідей державних службовців на запитання щодо того, до кого вони зверталися або з ким ділилися своїми переживаннями після епізодів онлайн-агресії, дозволяє оцінити рівень довіри до різних соціальних і професійних середовищ, а також сформулювати висновки про ступінь відкритості респондентів у ситуаціях цифрового психологічного впливу (табл. 2.17).

Найвищий рівень довіри продемонстровано щодо неформального особистого оточення — родини та друзів. Зокрема, 57,9% респондентів (34,5% згодні, 23,4% повністю згодні) погоджуються з тим, що обговорювали події, які їх засмутили в Інтернеті, з членами родини. Ще вищий показник довіри зафіксовано щодо друзів: 64,8% опитаних (43,2% згодні, 21,6% повністю згодні) відкрито ділилися з ними переживаннями. Це свідчить про ключову роль особистісно значущих контактів у подоланні наслідків кіберхейту.

Натомість показники звернень до професійного середовища є істотно нижчими. Лише 19,1% респондентів погоджуються, що обговорювали пережите з колегами, і лише 13,9% — з керівництвом. При цьому понад 80%

опитаних (38,3% + 42,3%) не погоджуються із твердженням про відкритість у колективі, а 86% (38,1% + 47,9%) — не зверталися до керівництва. Це вказує на наявність професійних бар'єрів щодо теми кібербезпеки, зокрема страху втратити репутацію, знижену довіру або стигматизацію.

Таблиця 2.17

Стан довіри та відкритості державних службовців щодо теми кіберхейту в кіберпросторі (%)

	абсолютно не згоден	***не згоден***	***важко відповісти***	***згоден***	***повністю згоден***
Члени сім'ї / родичі	19,4	22,5	0,2	34,5	23,4
Друг/подруга	15,2	19,3	0,7	43,2	21,6
Колеги	38,3	42,3	0,3	11,3	7,8
Керівництво	38,1	47,9	0,1	9,4	4,5
Терапевт / психолог / лікар	41,8	51,3	0,7	3,4	2,8
Поліція	40,9	52,2	0,3	3,7	2,9
Онлайн-портал допомоги та довіри	32,1	43,8	1,8	11,7	10,6
Психологічні консультаційні центри / Телефон довіри	37,9	39,7	1,5	11,4	9,5
Ніхто	15,5	17,8	0,4	41,8	24,5

Вкрай низький рівень відкритості продемонстровано щодо інституційних та спеціалізованих структур допомоги. Звернення до психологів, терапевтів чи лікарів підтвердили лише 6,2% респондентів (3,4% згодні, 2,8% повністю згодні), а до поліції — 6,6%. Більшість (понад 90%) взагалі не зверталися до таких джерел допомоги. Аналогічна ситуація фіксується і щодо онлайн-порталів довіри (22,3% позитивних відповідей) та телефонів довіри чи консультаційних центрів (20,9% згодні або повністю згодні).

Показово, що найбільша сукупна підтримка отримала відповідь «Ніхто» — 66,3% респондентів (41,8% згодні, 24,5% повністю згодні) визнали, що не ділилися з жодним із зазначених суб'єктів своїм негативним досвідом. Така поведінка свідчить про високий рівень внутрішньої замкненості, недовіри до

зовнішньої допомоги або ж відсутності сформованої культури звернення по підтримку в ситуаціях цифрової агресії.

Узагальнено результати дозволяють зробити висновок, що у випадках кіберхейту державні службовці орієнтовані переважно на внутрішні ресурси подолання стресових ситуацій або на нормативно прийнятні приватні соціальні зв'язки, тоді як професійне середовище і спеціалізовані служби сприймаються як мало доступні або недоречні для подібних комунікацій (рис. 2.25).

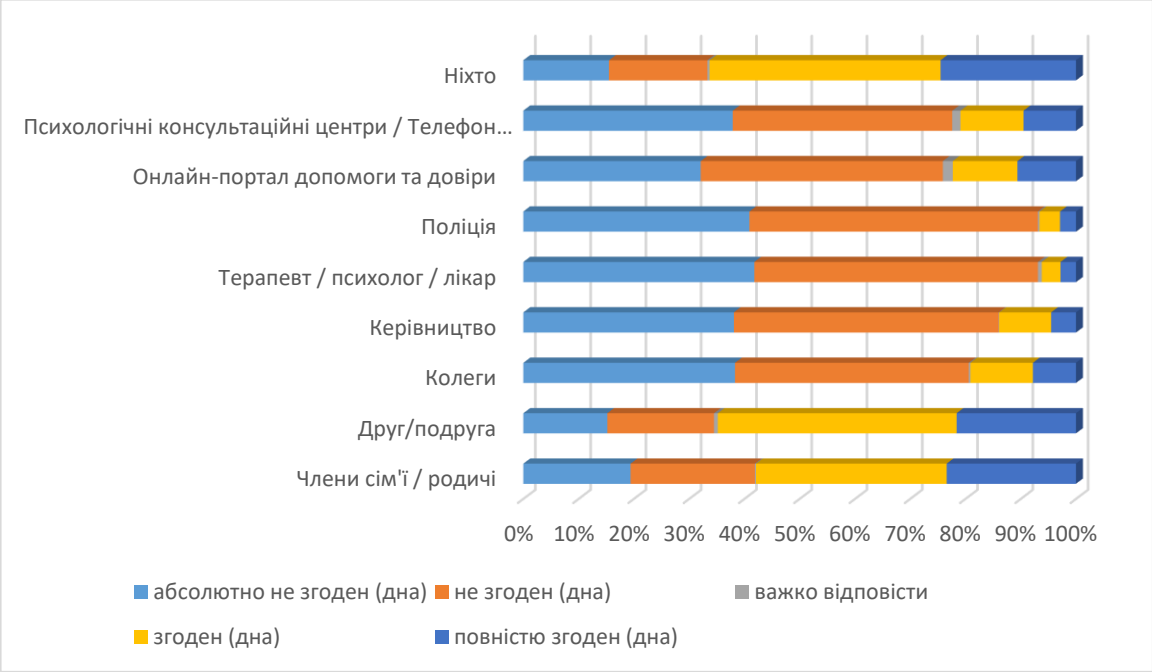

Рис. 2.25. Подолання стресових ситуацій державними службовцями у кіберпросторі (%).

Це підтверджує необхідність розробки програм підвищення рівня довіри до інституцій допомоги, популяризації культури психологічної підтримки в органах державної влади та впровадження механізмів раннього реагування на кіберзагрози в робочому колективі.

Крім того проаналізувавши відповіді державних службовців щодо бажаних форм підтримки у випадку зіткнення з проявами кіберхейту ми змогли виокремити основні напрями очікуваної допомоги та окреслити рівень

усвідомлення потреби у зовнішній підтримці у цифровому середовищі (рис. 2.26).

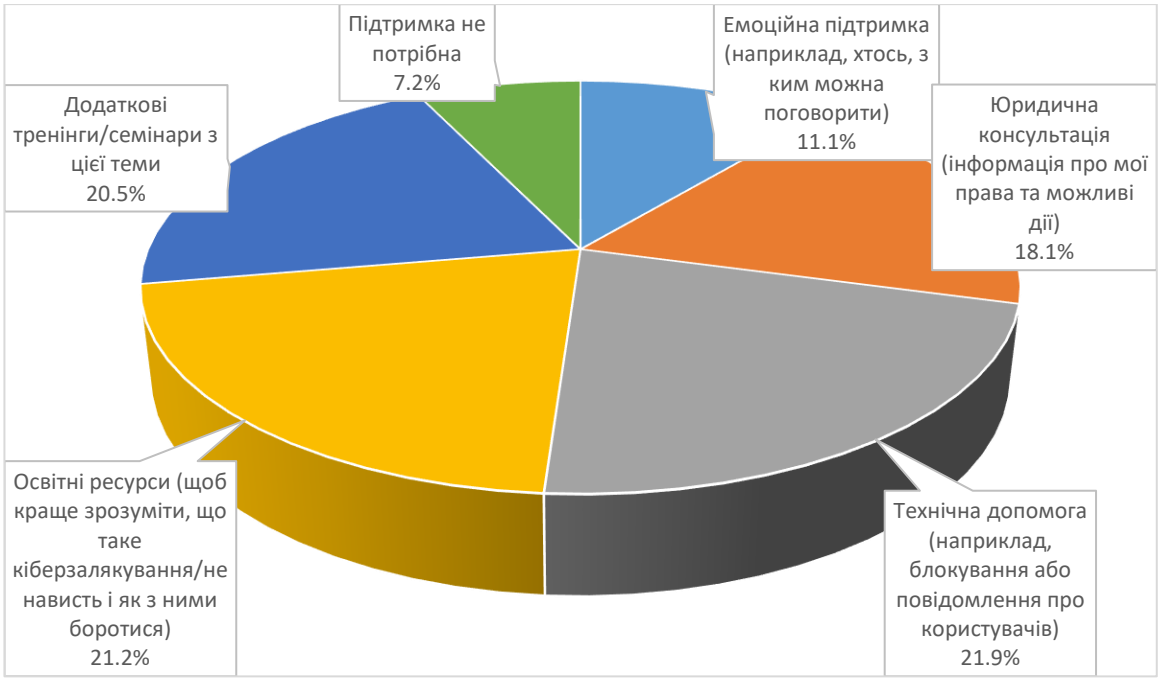

Рис. 2.26. Бажані форми підтримки у випадку зіткнення з проявами кіберхейту (%).

Найбільшу частку відповідей отримала позиція, пов’язана з наданням технічної допомоги – 21,9% респондентів зазначили, що потребують допомоги у блокуванні агресивних користувачів, повідомленні про порушення або застосуванні інших технічних засобів цифрового захисту. Це свідчить про зростання обізнаності щодо практичних аспектів безпеки в Інтернеті та важливість розширення технічних навичок самозахисту серед державних службовців.

Дещо нижчі, але майже рівнозначні показники продемонстрували запити на освітні ресурси (21,2%) та додаткові тренінги/семінари (20,5%). Це свідчить про усвідомлення важливості системної підготовки у сфері цифрової безпеки, розуміння механізмів кібербулінгу та кіберхейту, а також потреби у формуванні алгоритмів поведінки в кризових ситуаціях у мережі. Сумарно майже 41,7% респондентів висловили бажання отримати саме освітньо-

інформаційну підтримку, що підкреслює значний потенціал для впровадження програм цифрової грамотності у системі державної служби.

Не менш важливою виявилася потреба у юридичній підтримці: 18,1% респондентів зазначили, що їм необхідна інформація про правові можливості захисту та дії у випадках онлайн-агресії. Це вказує на брак правової обізнаності щодо механізмів захисту від кібербулінгу та кіберзалякування, а також на потребу у доступних консультаційних ресурсах.

Водночас лише 11,1% респондентів висловили потребу в емоційній підтримці, тобто у можливості обговорення пережитого з іншими людьми. Це найнижчий показник серед усіх запропонованих варіантів, що може свідчити як про недостатню культуру звернення по психологічну допомогу, так і про стереотипне сприйняття кіберхейту як несуттєвої чи не вартої емоційної уваги проблеми.

Цікаво, що 7,2% опитаних заявили, що не потребують жодної підтримки у випадках кіберхейту. Ця частка свідчить або про високий рівень особистої стресостійкості, або про занижену оцінку ризиків, пов'язаних із цифровою агресією.

Узагальнюючи результати, можна зробити висновок, що державні службовці демонструють переважно прагматично-раціональну модель очікуваної допомоги у випадках кіберхейту, віддаючи перевагу технічним, юридичним та освітнім інструментам захисту. Водночас потреба в емоційній підтримці залишається найменш артикульованою, що вказує на необхідність формування більшої уваги до психологічних аспектів безпеки в кіберпросторі. Отримані дані підкреслюють актуальність розробки комплексних програм підтримки, що поєднуватимуть технічні, правові та психологічні складові для підвищення рівня цифрової стійкості державних службовців.

Аналіз відповідей державних службовців на запитання щодо того, чи розглядалася тема ненависті в Інтернеті у їхньому робочому середовищі, засвідчив недостатній рівень уваги до цієї проблематики у професійному контексті (рис. 2.27).

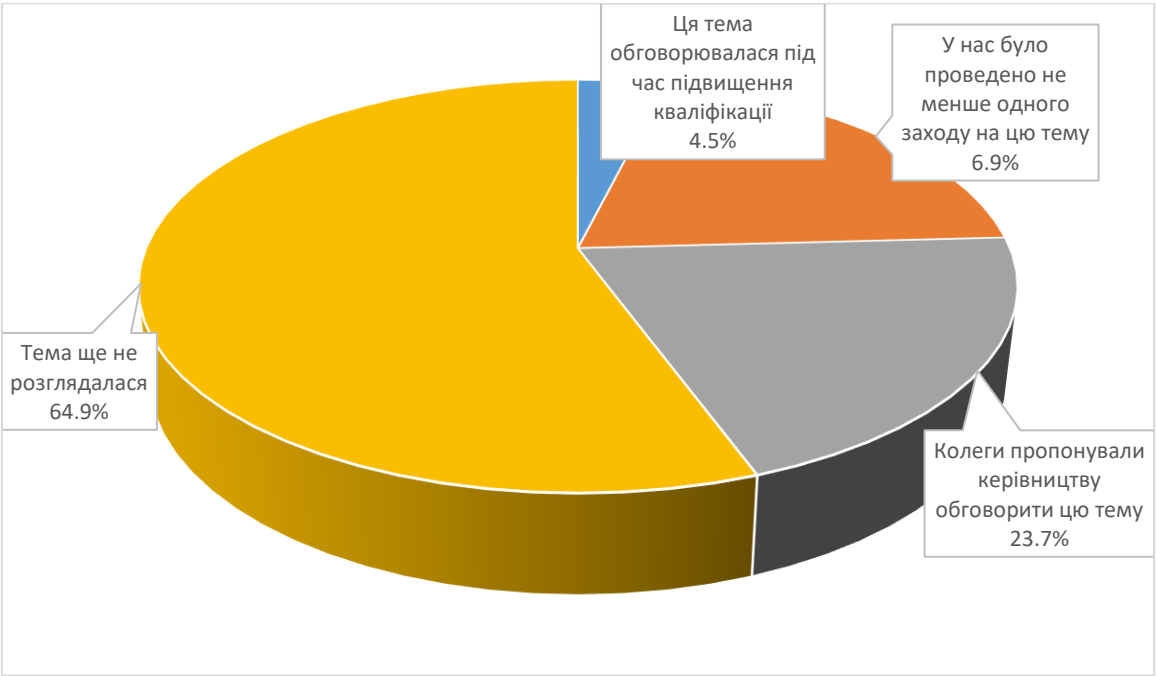

Рис. 2.27. Представлення теми кіберхейту в професійному середовищі (%).

Лише 4,5% респондентів зазначили, що питання кіберхейту порушувалося під час заходів з підвищення кваліфікації. Ще 6,9% опитаних вказали, що у їхніх організаціях було проведено щонайменше один захід, присвячений цій темі.

Водночас 23,7% державних службовців повідомили, що їхні колеги пропонували керівництву обговорити питання ненависті в Інтернеті, однак жодних заходів проведено не було. Переважна більшість респондентів – 64,9% – зазначили, що тема кіберхейту взагалі не піднімалася у межах їхнього робочого простору.

Отримані дані вказують на недостатню інтеграцію питань цифрової етики, інформаційної безпеки та психологічної стійкості до програм професійного розвитку державних службовців, що потребує негайної уваги з боку органів державної влади та системи державного управління загалом.

2.3. Чинники, що впливають на професійну діяльність державних службовців у кіберпросторі

В умовах цифрової трансформації державного управління кіберпростір стає не лише середовищем професійної діяльності державних службовців, а й чинником, що безпосередньо впливає на їхню ефективність, психологічний стан, комунікативну поведінку та здатність до прийняття рішень. Особливості взаємодії з цифровими платформами, динаміка онлайн-комунікації, інформаційне перевантаження, ризики кібербулінгу, а також розвиток цифрових звичок формують новий контекст професійної діяльності. У таких умовах критичне значення набуває аналіз чинників, які зумовлюють продуктивність, безпеку та психологічну стійкість державних службовців у мережевому середовищі.

До чинників, що можуть мати як позитивний, так і негативний вплив на службову діяльність у цифровому просторі, належать досвід взаємодії з кіберзагрозами, особистісні стратегії реагування, рівень цифрової компетентності, наявність підтримки від соціального оточення, ступінь самоконтролю в онлайновому середовищі, а також рівень довіри до інституцій. Їх вивчення дозволяє визначити потенційні зони ризику для професійної діяльності та запропонувати напрямки посилення адаптаційного ресурсу державних службовців.

Емпіричну основу цього пункту становлять узагальнені результати соціологічного дослідження, що проводилося з метою вивчення досвіду, ставлення та поведінкових практик державних службовців у кіберпросторі. Опитування дозволило виокремити низку чинників, що мають системний вплив на якість виконання посадових обов’язків, рівень цифрового навантаження, психологічну напруженість та організаційну ефективність.

У подальшому викладі буде здійснено структурований аналіз ключових груп чинників, які охоплюють індивідуально-психологічні, соціально-комунікаційні та організаційно-інституційні виміри. Кожен з них розкриває

певний аспект професійної взаємодії державних службовців із цифровим середовищем та визначає ступінь їхньої готовності ефективно діяти в умовах цифрової реальності.

Індивідіуально-психологічні чинники відіграють важливу роль у забезпеченні професійної ефективності державних службовців у кіберпросторі. Вони пов'язані як з індивідуальною чутливістю до цифрових загроз, так і з внутрішньою психологічною готовністю до реагування на виклики мережевого середовища, зокрема на прояви кіберхейту, інформаційного тиску, маніпулятивних комунікацій тощо.

Результати опитування показали, що емоційна реакція на кіберхейт серед державних службовців є досить інтенсивною. Зокрема, 49,5% респондентів зазначили, що часто зляться**,** стикаючись із проявами ненависті в інтернеті, ще 32,2% – періодично, а 10,1% – рідко. Схожим чином проявляється і реакція засмучення: 48,4% – часто, 25,9% – періодично, 14,8% – рідко. Ці дані свідчать про високу емоційну включеність державних службовців у ситуації онлайн-агресії.

Водночас частина респондентів демонструє емоційну дистанційованість: 64,8% заявили, що їм байдуже до проявів кіберхейту, а 69,1% не погоджуються з тим, що спостереження за подібними ситуаціями викликає у них сміх чи задоволення. Це може свідчити як про психологічний захисний механізм, так і про професійне відсторонення, властиве частині державних службовців.

Ще один показник емоційної взаємодії з цифровим простором – це відчуття безпорадності, яке декларували 17,9% респондентів часто, 20,2% – періодично, 28,9% – рідко, і лише 32,6% – ніколи. Такий розподіл засвідчує, що третина опитаних не має сформованої емоційної стійкості до деструктивного впливу віртуального середовища, що може негативно позначатися на їхній професійній активності та впевненості в прийнятті рішень. Також значним є рівень психологічної вразливості до проявів кіберзалякування. Дані свідчать, що 48,4% службовців часто засмучуються

через кіберхейт, 49,5% зляться, а 17,9% відчувають безпорадність. При цьому 12,1% визнають бажання помститися, що свідчить про емоційну нестабільність у відповідь на цифрову агресію. Однак водночас велика частка респондентів (64,8%) заявили, що їм «все одно», що може інтерпретуватися як психологічний захисний механізм уникнення або ознака емоційного вигорання.

Окрему увагу заслуговує емоційна мотивація до дії: 40,3% респондентів зазначили, що часто мають бажання протистояти кіберхейту, ще 20,1% – періодично, а 21,2% – рідко. Це свідчить про наявність значного потенціалу для активної позиції в захисті професійної та особистої гідності, проте вимагає належної підтримки та формалізованих механізмів реагування.

Психологічна стійкість, саморегуляція, рівень самооцінки та емоційне благополуччя є фундаментальними чинниками професійної ефективності державних службовців у цифровому середовищі. Оскільки кіберпростір не лише надає інструменти для роботи, але й створює умови для високого рівня стресу, емоційного виснаження, конфліктів та залучення до токсичних комунікацій, саме психологічні характеристики особистості відіграють критично важливу роль у збереженні професійної продуктивності.

Так, аналіз самооцінки державних службовців показав, що лише **17,3%** повністю задоволені собою, ще 19,5% частково згодні з цим твердженням. Водночас значна частина респондентів продемонструвала наявність негативної самооцінки: 28,4% зізнаються, що іноді вважають себе «поганими в усьому», 30,2% вказують, що їм «немає чим пишатися», а 23,3% почуваються невдахами. Більше половини респондентів **(**67,9%**)** періодично відчувають неефективність. Ці показники свідчать про високий рівень внутрішнього критицизму, що може підвищувати ризики вигоряння, знижувати впевненість у професійних рішеннях та загалом послаблювати здатність протистояти зовнішнім загрозам, зокрема в інтернет-середовищі.

Ці дані підтверджують необхідність посилення інституційної уваги до психологічної підтримки персоналу, зокрема через залучення психологів,

організацію тренінгів із саморегуляції, розвиток навичок конструктивного реагування на цифрові конфлікти, а також формування культури довіри в державних установах.

Загалом отримані результати дають підстави вважати, що психоемоційні чинники виступають одним із визначальних елементів у структурі професійної взаємодії державних службовців із цифровим середовищем. Формування емоційної стійкості, розвиток навичок саморегуляції та забезпечення психологічної підтримки є необхідною умовою ефективного функціонування службовця в умовах інформаційного тиску та цифрових загроз.

Соціально-комунікативні чинники, пов'язані з перебуванням державних службовців у кіберпросторі, формують контекст їхньої професійної ефективності, інформаційної дисципліни та цифрової відповідальності. Ці чинники визначають, якою мірою службовці здатні протистояти кіберзагрозам, дотримуватися етичних норм онлайн-взаємодії та забезпечувати належний рівень саморегуляції у віртуальному середовищі. Соціаотним контекстом тут виступають соціальні мережі, коментарі, месенджери та, навіть, онлайн-ігри, де більшість службовців стикалися з проявами кіберхейту.

Дані опитування свідчать про те, що значна частина державних службовців демонструє як активні, так і пасивні стратегії протидії (ігнорування, звернення до платформи, блокування, конфронтація), однак випадки звернення до офіційних інституцій (керівництва, поліції, фахових служб) залишаються поодинокими. Це зумовлює акцентування уваги на поведінкових чинниках державних службовцях у ситуаціях, пов'язаних із кіберхейтом.

Так, при виникненні подібних ситуацій 41,2% респондентів зізнаються, що мають бажання помститися, 27,4% – періодично**,** а 19,2% – рідко. Близько 31,3% також часто вступають у конфронтацію, захищаючи себе або інших, ще 28,9% – повністю згодні, що це є їхньою типовою реакцією. Такі дані можуть

свідчити про наявність імпульсивних стратегій поведінки, зумовлених емоційним напруженням або відсутністю чітких алгоритмів реагування.

Водночас частина респондентів демонструє пасивноуникаючу поведінку: 36,4% повністю або частково згодні з тим, що ніяк не реагують на хейт, 21,5% – закривають сайт чи застосунок, а 36,6% – на деякий час узагалі припиняють користування Інтернетом**.** Така реакція може бути наслідком втоми, небажання конфліктувати або зниження толерантності до цифрової агресії.

Іншим важливим поведінковим виявом є звернення по допомогу. Найчастіше респонденти обговорюють інциденти хейту з друзями (49,2%) і колегами (29,8%), рідше – повідомляють про контент на платформі (46,1%) або використовують технічні функції блокування (40,9%). Водночас звернення до поліції (26,2%) чи до керівництва (7,6%) є значно менш поширеним, що може свідчити про брак довіри до формальних інституцій або низький рівень організаційної підтримки.

Значущим поведінковим аспектом є також участь самих державних службовців у створенні або поширенні контенту, який може розцінюватися як агресивний або дискримінаційний. 23,9% респондентів визнали, що часто поширювали або створювали образливі повідомлення, 29,5% – періодично, ще 24,5% – рідко. Серед найчастіших мотивацій – конфлікт із іншими особами (48,3%), емоційні стани, як-от поганий настрій (47,2%) або бажання висловити свою думку (46,8%), а також помста за інших (31,2%).

Отже, поведінкові реакції державних службовців у кіберпросторі варіюються від активного протистояння та конфронтації до уникання, замовчування або навіть участі у поширенні агресивного контенту. Це свідчить про необхідність системного впливу на формування етичних стандартів онлайн-взаємодії, розвиток цифрових компетентностей і створення умов для безпечного реагування у випадках загрозливого контенту.

Крім того, було проаналізовано характер соціальної взаємодії в межах трудового колективу. Дані опитування демонструють недостатній рівень

психологічної відкритості та підтримки з боку колег. Лише 10,9% респондентів відчувають, що можуть вільно обговорювати свої погляди з колегами без збентеження; 9,5% задоволені якістю комунікації; 6,3% вказали, що можуть розповісти про свої проблеми. Натомість понад третина респондентів демонструє протилежну позицію – 33-36% абсолютно не погоджуються з цими твердженнями. Така міжособистісна ізольованість формує відчуття відчуження та ускладнює формування колективної емоційної підтримки.

Інформаційно-комунікаційна площина виявляє нерівномірне сприйняття цифрового простору, де значну роль відіграють політичні конфлікти, соціальні стереотипи, дискримінаційні теми. Політика, сексуальність, зовнішність, здоров'я, вік та економічний статус стають осередками агресії, яка має вплив на психологічний стан державних службовців і атмосферу в цифрових спільнотах.

Організаційно-інституційні чинники відіграють важливу роль у забезпеченні стійкості державних службовців до викликів кіберпростору, впливаючи на їхню здатність реагувати на кіберзагрози, зберігати продуктивність, а також формувати здоровий мікроклімат у трудовому колективі. Ці чинники охоплюють рівень підтримки з боку керівництва, наявність внутрішньої політики з цифрової безпеки, доступність навчання, функціонування механізмів інформування та зворотного зв'язку.

До організаційних чинників належать тривалість перебування в інтернеті під час робочого дня, рівень залучення до неслужбових активностей та цифрової прокрастинації. Високий рівень онлайн-присутності, що перевищує 5 годин у 31,2% респондентів, а також щоденне відволікання на сторонні цифрові дії у 41,3%, свідчать про потребу у вдосконаленні норм використання цифрового часу та регламентів професійної поведінки в інтернеті.

Результати опитування засвідчують обмежений рівень інституційної підтримки щодо питань кіберхейту. Так, лише 4,5% респондентів зазначили,

що тема ненависті в інтернеті розглядалася в межах підвищення кваліфікації, 6,9% підтвердили наявність хоча б одного заходу на цю тему в межах їхньої установи. Водночас 23,7% повідомили, що колеги пропонували обговорити цю проблему з керівництвом, однак 64,9% визнали, що тема кіберхейту на робочому місці ніколи не порушувалася. Це свідчить про низьку інституціалізацію тематики цифрової безпеки в державному управлінні.

Крім того, показники довіри до організаційного оточення є досить низькими. Лише 9,4% респондентів згодні або повністю згодні з тим, що можуть обговорити інциденти з керівництвом, і лише 11,3% – з колегами. Ще нижчими є показники звернення до зовнішніх організацій – поліції (6,6%) або психологічних центрів (10,5%). Також 41,8% вказали, що не звертаються до жодної особи чи інституції у випадку психологічного дискомфорту в інтернеті. Такі результати демонструють обмежений рівень горизонтальної та вертикальної підтримки в організаційному середовищі.

Низький рівень довіри до керівництва підтверджується і загальним рівнем довіри до інституцій. Лише 13,4% державних службовців висловили «високий рівень довіри» до свого керівника, тоді як 28,6% відверто не довіряють йому, а 36,8% залишаються невпевненими. Подібна картина спостерігається і щодо довіри до правової системи, поліції, а також ЗМІ, що знижує ймовірність використання офіційних каналів реагування у разі загроз з кіберпростору.

Також виявлено суттєвий брак практичних інституційних заходів. Попри наявність потреби у підтримці (зокрема, 21,9% респондентів виявили запит на технічну допомогу, 20,5% – на тренінги, 18,1% – на юридичні консультації), системна відповідь на ці потреби з боку організацій відсутня або реалізується на низькому рівні.

Отже, організаційно-інституційні чинники залишаються одним із найслабших місць у системі професійної підтримки державних службовців у кіберпросторі. Підвищення уваги до цифрової безпеки з боку керівництва, впровадження інституційних механізмів інформування, консультування, а

також нормативне врегулювання питань реагування на цифрову агресію мають стати пріоритетом у державній політиці.

Загалом результати дослідження дозволяють дійти висновку, що ефективна діяльність державного службовця в кіберпросторі залежить не лише від технічної обізнаності, а й від сформованих стратегій поведінки, підтримки організаційного середовища, а також рівня емоційної зрілості, довіри й солідарності в професійному середовищі. Відтак, підвищення готовності до діяльності в умовах цифрової трансформації має ґрунтуватися на інтеграції організаційних, освітніх, психологічних і комунікаційних підходів.

Висновки до розділу 2

Проведене теоретико-емпіричне дослідження дозволило комплексно охарактеризувати стан готовності державних службовців до професійної діяльності в умовах цифровізації, а також визначити ключові проблеми, пов’язані з їхньою взаємодією в кіберпросторі. Встановлено, що професійна активність державних службовців у цифровому середовищі супроводжується як новими можливостями для ефективної комунікації, так і зростанням соціальних ризиків, насамперед – кіберзалякуванням, кіберхейтом, прокрастинацією та цифровою втомою.

Опитування підтвердило, що значна частина державних службовців регулярно перебуває в інтернет-просторі не лише з професійною, а й з особистою метою. Водночас понад 40% з них зізналися у щоденному відволіканні на неслужбові онлайн-активності, а майже 22% постійно відкладають виконання службових завдань на користь другорядного цифрового контенту. Це вказує на поширення діджитал-прокрастинації як деструктивного чинника, що знижує продуктивність та ускладнює самоменеджмент державного службовця.

Однією з найгостріших проблем виявилося поширення кіберхейту – зневажливих висловлювань, принижень і ворожих дій у соціальних мережах, месенджерах, чатах і навіть у приватних повідомленнях. Кіберхейт часто стосується політичних тем, зовнішності, соціального статусу, гендеру, сексуальної орієнтації. Більшість респондентів визнають, що ці прояви викликають сильну емоційну реакцію: злість, засмучення, тривожність, що ускладнює збереження психологічної стійкості під час професійного функціонування.

Окрему загрозу становить не лише переживання кібернасильства, а й участь самих держслужбовців в агресивних діях у кіберпросторі. Значна частина респондентів зізналася у поширенні образливого контенту, що є показником цифрової незрілості, низької етичної стійкості та потреби в нормативній регуляції поведінки в мережі.

Виявлено також низький рівень інституційної довіри: респонденти не готові звертатися до керівництва, поліції чи психологічних служб у випадку кіберконфлікту, натомість переважно покладаються на неформальні джерела підтримки – друзів, родину або ні на кого. Це свідчить про потребу створення механізмів внутрішньої підтримки, підвищення довіри до служб безпеки та розвитку психологічної компетентності.

Серед запитів на підтримку переважають освітні (тренінги, інформаційні ресурси), технічні (блокування, налаштування безпеки) та юридичні потреби. Це вказує на важливість формування інституційних програм цифрової обізнаності та професійної підготовки в контексті кібербезпеки.

Таким чином, професійна діяльність державних службовців у кіберпросторі детермінується сукупністю чинників: індивідуально-психологічних, соціально-комунікативних та організаційно-інституційних. Їх врахування є критично необхідним для формування цілісної системи цифрової адаптації та безпеки державної служби в умовах сучасних викликів.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ПЕРСОНАЛОМ НА ДЕРЖАВНІЙ СЛУЖБІ

Результати соціологічного дослідження, представлені в попередньому розділі, засвідчили, що цифрове середовище значною мірою впливає на професійну поведінку, психологічний комфорт і ефективність державних службовців. Поширення кібербулінгу, зниження довіри, прокрастинація, брак підтримки та відсутність сталої комунікаційної культури – усе це потребує системного втручання з боку державної кадрової політики.

У цьому контексті соціальна інженерія як інструмент стратегічного управління персоналом дозволяє застосовувати моделі поведінкової оптимізації, побудови довіри та формування кіберкомпетентностей. Третій розділ дисертаційного дослідження спрямований на обґрунтування напрямів удосконалення системи управління державними службовцями з урахуванням міжнародного досвіду, реальних потреб персоналу та специфіки взаємодії в кіберпросторі.

3.1. Імплементація кращих міжнародних практик щодо удосконалення взаємодії державних службовців у кіберпросторі

У сфері державного управління соціальна інженерія може розглядатися як ефективний інструмент формування, регуляції та вдосконалення цифрової поведінки державних службовців. Вона охоплює систематичне впровадження психологічних, комунікативних та соціальних впливів, які спрямовані на адаптацію персоналу до цифрового середовища, розвиток цифрової етики та профілактику кіберзагроз.

У класичному трактуванні, соціальна інженерія найчастіше асоціюється з кібератаками, які використовують психологічні методи впливу на людей з

метою отримання доступу до конфіденційної інформації. У кібербезпековому аспекті соціальна інженерія виступає ключовим ризиком – зловмисники впливають на емоції користувача, викликаючи страх або довіру, щоб маніпулювати його поведінкою [264; 292].

Утім, як доводить практика Behavioural Insights Team (BIT) у Великій Британії, ці самі механізми можна адаптувати в інтересах організаційного розвитку. Наприклад, BIT впроваджує технології "nudge" – м'якого підштовхування – для формування бажаної поведінки працівників шляхом зміни архітектури вибору або інформаційного середовища. Ці підходи використовувалися для покращення дисципліни, підвищення дотримання етичних стандартів та запобігання конфліктам у державному секторі [221].

Світовий банк пропонує розглядати соціальну інженерію як інструмент боротьби з ризиками корупції та зловживаннями через систематичний вплив на соціальні установки та організаційну культуру в державному секторі. Це досягається шляхом інституціоналізації прозорих правил, створенням систем заохочення етичної поведінки та інтеграцією психологічних інтервенцій у політику управління персоналом.

Якщо соціальна інженерія розглядається як інструмент трансформації кадрової політики, то вона передбачає застосування соціально-психологічних механізмів для моделювання поведінки державних службовців. Це може здійснюватися різними шляхами:

1. Однією з ключових концептуальних основ моделювання цифрової поведінки в межах соціальної інженерії є Теорія запланованої поведінки (Theory of Planned Behavior, TPB) запропонована І. Айзеном [211]. Згідно з цією теорією, реальна поведінка індивіда визначається його намірами, які, у свою чергу, формуються під впливом трьох основних чинників:

– особистісної установки до поведінки, тобто оцінки індивідом наслідків виконання певної дії;

– суб’єктивних соціальних норм, включно з інжунктивними (соціально-схвалюваними) і дескриптивними (типовими в межах соціальної групи) очікуваннями;

– сприйнятого поведінкового контролю, який відображає впевненість особи у власній здатності реалізувати намічену дію за наявних умов.

У контексті публічного управління особливої значущості набуває саме компонент соціальних норм, оскільки цифрова поведінка державних службовців часто залежить від загальноприйнятих (або негласних) стандартів, що функціонують у межах професійної спільноти. Як зазначають дослідники в галузі поведінкових наук, групові норми і колективні установки можуть виступати потужним інструментом корекції індивідуальної поведінки у бік більш відповідального та етичного цифрового самовираження [224].

Таким чином, застосування інструментарію ТРВ у сфері державної служби дозволяє не лише оцінити наявні моделі поведінки, а й розробити ефективні поведінкові інтервенції, орієнтовані на зміну установок та норм із метою формування сталих практик безпечної й доброчесної комунікації в цифровому середовищі.

2. Найефективніших механізмів соціальної інженерії в межах публічного управління є моделювання етичної поведінки через соціальні норми. Такий підхід реалізується за допомогою технології «social norm nudging» («підштовхування соціальних норм») – м’якого підштовхування до певної дії шляхом апеляції до колективних уявлень про соціально бажану поведінку. Цей інструмент передбачає не пряме примусове регулювання, а формування етичної атмосфери за рахунок таких компонентів:

- демонстрація типового зразка поведінки (наприклад, «переважна більшість співробітників дотримується цифрового етикету»);

- підкреслення соціального схвалення або позитивного підкріплення бажаної дії (наприклад, «поважна цифрова комунікація підвищує авторитет служби»).

Згідно з результатами досліджень, соціальні норми особливо ефективні тоді, коли вони подаються у формі інформування про поведінку «більшості» або «типових колег» [221]. Такий ефект був зафіксований у численних експериментах. Зокрема, в Німеччині використання порівняльної інформації щодо споживання електроенергії між домогосподарствами виявилось потужним чинником зміни поведінки в бік більш енергоощадної моделі [229].

У контексті цифрової поведінки державних службовців технологія «підштовхування соціальних норм» може бути реалізована через впровадження візуалізованих етичних стандартів, кейсів позитивних практик або соціальних кампаній із просування доброчесного цифрового спілкування в середині органів державної влади. Це дозволяє створити ефект соціального тиску, що підвищує дотримання нових етичних норм без необхідності жорстких адміністративних санкцій.

3. Також у сучасних підходах до управління поведінкою персоналу дедалі більшого значення набуває концепція «advisory nudging» («консультативне або порадницьке підштовхування») – це також вид м’якого впливу, що поєднує інформаційний супровід із повагою до автономії індивіда. На відміну від директивних чи маніпулятивних стратегій, «консультативне підштовхування» не обмежує вибір, а сприяє усвідомленому прийняттю рішень, активуючи внутрішні цінності, відповідальність і рефлексивність особистості [317; 323].

У сфері державного управління, зокрема в HR-контексті, такий підхід має потенціал для формування етичної цифрової поведінки, оскільки реалізується шляхом:

– ненав’язливих нагадувань про внутрішні цифрові політики та стандарти;

– демонстрації прикладів етичної комунікації, які викликають бажання наслідувати поведінку колег;

– інформаційного дизайну середовища, де пріоритетними стають дії, що відповідають нормам професійної доброчесності (наприклад, автоматично встановлені параметри конфіденційності, підказки до стилю повідомлень);

– візуалізації наслідків онлайн-поведінки (наприклад, анонімні кейси негативного впливу цифрових висловлювань на репутацію інституцій).

Практичні реалізації цього інструменту засвідчені, зокрема, у досвіді Сінгапуру та Данії, де «консультативне підштовхування» використовується в державних кампаніях із цифрової етики та в системах професійного розвитку державних службовців [223; 269]. Наприклад, у Сингапурі у межах урядової кампанії «Sustainability Starts with Me» співробітники Міністерства навколишнього середовища створювали персональні «зони сортування відходів» або нагадування наприкінці дня, які слугували своєрідними «самопідказками» («self-nudge») для підтримки екологічних звичок (наприклад, сортування, миття пляшок). Такий підхід демонструє, як м’які підказки без примусу сприяють формуванню відповідальної поведінки без директивного контролю [283].

Крім того, Міністерство праці Сінгапуру (MOM) вдосконалило формат нагадувальних листів для роботодавців. Було: спрощено текст, додано соціальне повідомлення «96 % роботодавців сплачують обов’язкові внески вчасно», листи надсилалися рожевим кольором, що психологічно відрізняло їх від звичайних. У результаті була покращена дисципліна сплати податків – на 3-5% більше роботодавців виконали зобов’язання вчасно, порівняно з попередньою кампанією [327].

У Данії в 2002 році був створений MindLab – інноваційна лабораторія при кількох міністерствах, яка спеціалізується на дизайн-мисленні, прототипуванні та моделюванні взаємодій між держслужбовцями та громадянами. Хоча це не класична модель «nudge», але її методологія – включаючи тестування поведінкових сценаріїв та соціального впливу – резонує з принципами «консультативного підштовхування» [325]. Наприклад, створення інформаційного простору, де колеги обговорюють прийом

цифрової етики, стимулює прийняття таких норм у щоденній практиці службовців. Подібний підхід застосовувався податковим агентством SKAT, яке замість типових бюрократичних презентацій, впроваджувало зустрічі стартапів із досвідченими підприємцями як джерелом довіри і прикладу [236]. Існує офіційне кейс-стаді від компанії Pensaki, в якому представлено результати впровадження даної методології іпотечною кампанією BRF-Kredit, яка отримала понад 90 % відгуків завдяки тому, що надсилала ручні конверти без логотипа, що викликало менший психологічний бар'єр у клієнтів з фінансовими труднощами [303]. Це можна сприймати як етичний механізм комунікації, що суттєво відрізняється від типового офіційного листування.

Таким чином, досвід цих країн свідчить, що застосування технологій поведінкового моделювання, зокрема через механізм «м'якого підштовхування», може стати ефективним інструментом трансформації професійної поведінки державних службовців. На відміну від директивних або каральних заходів, цей підхід базується на засадах поваги до автономії особистості та ґрунтується на етичних принципах добровільного вибору в межах структурованого інформаційного середовища.

У контексті державної служби України ці практики можуть бути адаптовані у формі методичної моделі «дизайну поведінки» для кадрових і комунікаційних стратегій. Зокрема, у цьому контексті доцільно:

- впровадити автоматизовані електронні повідомлення із вбудованими соціальними меседжами («80% колег уже пройшли тренінг з кібергігієни»);

- використовувати візуальні підказки (кольорові маркування, шаблони формулярів) для посилення уваги до регламентів;

- впроваджувати структуровану подачу інформації у внутрішніх комунікаціях, що нормалізує бажані моделі поведінки;

- розробити інформаційно-психологічне середовище (наприклад, дашборди, внутрішні інтерфейси) з вбудованими нагадуваннями про цифрову доброчесність і професійну етику.

Таким чином, застосування концепції «м'якого підштовхування» у державному управлінні дасть можливість підняти ефективність у формуванні цифрової культури поведінки. Її імплементація в українській системі державної служби є перспективним напрямом, що дозволить без надмірного адміністративного тиску формувати етично виважене, соціально відповідальне та проактивне цифрове середовище.

Також із зростанням ролі цифрових платформ у діяльності державного сектору та посиленням кіберзагроз, питання цифрової етики набуває принципового значення в системі державного управління. Цифровий етичний кодекс розглядається як інструмент нормативного регулювання поведінки державних службовців у кіберпросторі, які здійснюють професійну взаємодію через соцмережі, електронну пошту, месенджери тощо, що у свою чергу забезпечує баланс між професійною відповідальністю, інформаційною безпекою та правами громадян.

У світовій практиці цифрові етичні кодекси (Digital Ethics Codes) є частиною більш широких рамок політики good governance, які базуються на прозорості, підзвітності та повазі до приватності в цифровому середовищі.

Так, Організація економічного співробітництва та розвитку (Organisation for Economic Co-operation and Development, OECD) у своєму документі *«Рамки політики цифрового урядування»* (*Digital Government Policy Framework,* 2020) підкреслює, що етичність, прозорість та інтегритет є фундаментальними принципами для побудови довіри між державними службовцями та громадянами [298]. Зокрема, OECD рекомендує урядам інтегрувати етичні стандарти у сферу цифрової державності, включаючи протидію поширенню дезінформації, забезпечення відкритості та поваги до приватності даних [295; 296].

Європейська Комісія в контексті політики «Цифровий компас 2030» (*Digital Compass 2030,* 2021) також акцентує увагу на фундаментальних цифрових правах і принципах, серед яких – прозорість, участь громадян, інклюзивність та захист від цифрової агресії. Документ окреслює вектор, в

якому держава має діяти для розбудови довіри до цифрової трансформації [241].

Рекомендації OECD та Європейської комісії (2021) також наголошують на необхідності адаптації професійних етичних стандартів до цифрової взаємодії, зокрема шляхом включення таких принципів, як: цифрова доброчесність (integrity), кіберетикет (netiquette), повага до інформаційного суверенітету особи, запобігання поширенню дезінформації та токсичного контенту.

Аналіз кращих міжнародних практик щодо удосконалення взаємодії державних службовців у кіберпросторі серед різних країн дав можливість виявити найефективніші та найпродуктивніші з них. Так, найуспішнішим прикладом врегулювання цифрової поведінки державних службовців вважається досвід ***Нідерландів***, де був розроблений окремий Кодекс поведінки щодо використання соціальних мереж державними службовцями (Code of Conduct for the Use of Social Media by Civil Servants) [290]. Цей документ є частиною ширшої етики публічної служби та має нормативно-роз'яснювальний характер, а також:

- визначає чіткі межі публічної активності державних службовців у соціальних мережах;

- поширюється на приватні акаунти, якщо висловлювання можуть бути інтерпретовані як позиція державної установи;

- охоплює позаробочий час, визнаючи, що навіть у неробочий період службовець залишається представником інституції;

- заохочує до відкритої комунікації, однак вимагає уникнення критики політичного керівництва, недопущення дискримінації чи мови ворожнечі;

- доповнюється регулярними освітніми семінарами, етичними кейсами, оновлюваними гайдлайнами та інформаційною підтримкою від HR-департаментів.

Цей досвід показує приклад успішного балансу між свободою самовираження та дотриманням професійної доброчесності. Застосування

такого підходу дозволяє зменшити ризики репутаційних втрат для державних інституцій і водночас зберегти довіру громадськості.

У ***Великій Британії*** діє чітке регламентування цифрової поведінки державних службовців через різні офіційні джерела. Основними серед них є: Рекомендації щодо соціальних мереж для державних службовців, Концепція SAFE та Цифрова комунікація.

«Рекомендації щодо соціальних мереж для державних службовців» є офіційною позицією уряду щодо того, як державні службовці повинні поводитися в соціальних мережах, включаючи особисті акаунти [257]. Ключові принципи:

- неупередженість і об'єктивність: державні службовці повинні уникати публікацій, які ставлять під сумнів їхню політичну нейтральність або авторитет органів влади.

- конфіденційність: заборонено публікувати службову інформацію, навіть якщо вона здається незначною.

- приватність – не захищеність: мається на увазі, що повідомлення у «приватних» чатах, групах або повідомленнях також підпадають під стандарти офіційної поведінки.

- поведінка в позаробочий час: навіть за межами робочого часу держслужбовець зобов’язаний дотримуватися професійних стандартів.

Дотримання норм поведінки в цифровому середовищі та соціальних мережах посідає особливе місце у професійних стандартах державної комунікації. Ці положення насамперед стосуються фахівців з цифрової комунікації та працівників комунікаційних підрозділів органів державної влади. Тому одним із ключових підходів до регулювання цифрової активності є концепція SAFE, яка включає такі складові:

- Розмежування (Separate) – чітке відділення особистого спілкування в мережі від професійної діяльності;
- Оцінка (Assess) – усвідомлений аналіз можливих ризиків перед публікацією повідомлень у цифровому просторі;

- Достовірність (Factual) – опора на перевірену інформацію та фактичну точність поширюваного контенту;
- Етичність (Ethical) – дотримання етичних норм і принципів, передбачених Кодексом державного службовця [256].

Згідно з цими принципами, усі дії представників державної служби в соціальних мережах, навіть здійснені в особистому порядку, повинні відповідати високим стандартам публічної поведінки. Необхідно враховувати, що будь-яка цифрова комунікація потенційно сприймається як позиція офіційної установи, що вимагає від державного службовця підвищеного рівня відповідальності.

«Цифрова комунікація» (Digital communication) – це більш прикладна інструкція для фахівців з комунікацій, яка встановлює стандарти для:

- управління цифровими каналами;
- моніторингу коментарів і реагування на них;
- розбудови позитивного цифрового іміджу інституції;
- контролю над тонами і стилем офіційних комунікацій.

Документ підкреслює, що навіть у публічних суперечках державний службовець має діяти стримано, доброзичливо і професійно [255].

Досвід ***Канади*** регламентується документом “Найкращі практики для державних службовців щодо особистого використання соціальних мереж” (Best Practices for Public Servants on Their Personal Use of Social Media, Government of Canada), який є офіційним керівництвом, що визначає правила та етичні стандарти поведінки для державних службовців Канади під час особистого користування соціальними мережами [258]. Його основна мета – забезпечити збереження публічної довіри до державної служби, гарантувати нейтральність та уникнути конфлікту інтересів у цифровому середовищі.

Ключові положення документа:

1. Політична нейтральність. Державні службовці зобов’язані утримуватись від:

- участі в онлайн-дискусіях, що мають політичне забарвлення;

- поширення або «лайків» публікацій, які можна інтерпретувати як підтримку певної політичної сили;

- коментування урядових рішень, якщо це може вплинути на сприйняття об'єктивності служби.

2. Конфіденційність та професіоналізм. Працівники не повинні:

- розголошувати інформацію, отриману під час виконання службових обов’язків;

- робити публічні заяви, які можуть підірвати довіру до державної служби;

- використовувати робочі дані або ресурси у персональних акаунтах.

3. Розмежування особистого та професійного. Документ наголошує, що навіть особисті акаунти у соцмережах можуть асоціюватися з професійним статусом. Тому:

- рекомендується мати чітке розділення між професійною і приватною присутністю онлайн;

- бажано уникати заяв, які можуть бути витлумачені як позиція урядового відомства.

Також в документі зазначається, що хоча державні службовці мають право на свободу вираження, це право не є абсолютним у контексті їхньої професійної ролі. Потрібно балансувати між особистою думкою та службовими обов’язками.

Попри відсутність окремого нормативного акту, який би безпосередньо регламентував цифровий етикет державних службовців у ***Естонії***, сформована національна модель управління цифровими комунікаціями в публічному секторі відзначається системністю, інституційною узгодженістю та інтеграцією етичних принципів у щоденну адміністративну практику. Центральним елементом цієї моделі є Кодекс етики державного службовця (Estonian Officials' Ethics Code), який, хоч і не фокусується виключно на поведінці у цифровому середовищі, містить низку норм загального характеру, релевантних до онлайн-взаємодій: вимоги доброчесності, нейтральності,

утримання від дискредитації органу влади, а також дотримання професійної лояльності [308].

Окрему увагу приділено питанню відповідальності службовців у соціальних мережах. Так, Рада з етики державних службовців (Public Service Ethics Council) у своїх рекомендаціях акцентує на тому, що особиста участь службовця у публічних дискусіях – зокрема в цифровому просторі – не повинна суперечити його посадовим обов'язкам і загальним етичним стандартам. У цьому контексті поведінка в соціальних мережах трактується як продовження офіційної публічної ролі службовця [274]. Зазначається, що навіть за використанням приватного акаунту, державний службовець несе етичну відповідальність за зміст висловлювань, які можуть бути ідентифіковані як пов'язані з його службовим статусом [289].

На інституційному рівні, усі міністерства та центральні органи виконавчої влади зобов'язані розробляти власні політики цифрової комунікації, включаючи рекомендації щодо ведення офіційних сторінок у соціальних мережах, способів реагування на публічну критику, а також процедур модерації вмісту. Ці політики затверджуються у межах внутрішніх регламентів та перебувають у компетенції PR-відділів відповідних установ [243].

Комплексну підтримку в розбудові цифрової етики надає також Національний центр кібербезпеки Естонії (NCSC-EE), який провадить просвітницькі кампанії (наприклад, «Ole IT-vaatlik»), спрямовані на підвищення цифрової обізнаності та формування навичок безпечної поведінки в інтернеті. Хоча ці ініціативи орієнтовані на широку громадськість, державні службовці також охоплюються цими заходами, зокрема через участь у тренінгах з цифрової гігієни [274].

Загалом, естонська модель демонструє, що навіть за відсутності спеціалізованого кодексу цифрового етикету, можливо досягти високого рівня етичної регуляції онлайн-поведінки державних службовців шляхом поєднання загальних етичних норм, інституційних політик, а також освітньо-

просвітницьких ініціатив. Такий підхід забезпечує адаптивність до динаміки цифрового середовища без створення надмірного регуляторного тиску.

Досить впливовим є Кодекс стандартів та поведінки державних службовців ***Ірландії*** (Civil Service Code of Standards and Behaviour) [238], у якому визначено ключові принципи діяльності державних службовців – доброчесність, неупередженість, законність і відповідальність – а також встановлено заборону участі в політичних акціях або висловлюваннях, навіть у позаробочий час, без спеціального дозволу. Кодекс є частиною умов працевлаштування та підлягає обов'язковому ознайомленню нових працівників. Крім того, існує Циркуляр 19/2009 «Державні службовці та політична діяльність», в якому у пункті 14 конкретно зазначено, що державні службовці, крім тих, хто належить до категорій, звільнених у пункті 13, не повинні публічно виступати з питань місцевих або національних політичних суперечок або висловлювати свої погляди з таких питань у засобах масової інформації (включаючи електронні ЗМІ та пресу) або в книгах, академічних роботах, статтях чи брошурах [237].

У 2020 році уряд ***Болгарії*** ухвалив повністю оновлений Кодекс поведінки державних службовців (ПМС № 57 від 2 квітня 2020 р., опублікований у «Държавен вестник», № 33 від 7 квітня 2020 р.), який вступив у силу 8 травня 2020 р. [235].

Кодекс визначає ключові етичні принципи, обов'язкові для службовців:

- законність – виконання обов'язків у межах конституційного та законодавчого поля;
- лояльність – відношення до інституції з повагою, уникання необґрунтованої критики;
- добросовісність, безпристрастність, рівноправність, відповідальність, конфіденційність, політична нейтральність – усі ці принципи зафіксовані у цьому документі як обов'язкові норми поведінки

Найважливішим для нашого дослідження виявилася Глава шоста («Особиста поведінка»), яка містить прямі вказівки щодо використання технологій і соціальних мереж:

Чл.17(1-2) – держслужбовці зобов'язані уникати будь-якого поведінкового прояву, в тому числі в цифровому середовищі, який може знизити престиж держслужби; також неприпустима поведінка, яка суперечить нормам цього Кодексу навіть поза межами робочого місця.

Чл.17(3) – працівники мають уникати будь-яких конфліктних ситуацій, контролюючи свої дії й утримуючись від емоційної реакції навіть у мережі.

Кодекс також передбачає чіткі рамки дисциплінарної відповідальності за порушення цифрових норм. Так, соціальні медіа згадуються в додаткових уточненнях як комунікаційні платформи, які підпадають під дію Кодексу, включно з публікаціями, спілкуванням і контентом, що може вплинути на репутацію держоргану [103; 104].

У лютому 2021 року уряд ***Індії*** впровадив комплекс нових правил, покликаних забезпечити етичну поведінку онлайн-платформ та цифрових медіа [326]. Журнали та інтернет-посередники (соціальні мережі, новинні ресурси, OTT сервіси) отримали чіткі обов'язки щодо контролю контенту, відповідальності за нього та підтримки користувацьких прав.

Основними концептами документу є:

1. Належна обачність: всі платформні оператори (Intermediaries) повинні публічно ввести посилання на правила використання, політику конфіденційності та користувацьку угоду; при порушенні умов, сервіс має право терміново припинити доступ або видалити контент.

2. Режим великих соціальних мереж (Significant Social Media Intermediaries, SSMI): платформи з великою кількістю зареєстрованих користувачів зобов'язані призначати головного відповідального за дотримання політик (Chief Compliance Officer), контактну особу для жалоб (Grievance Officer) та механізм перевірки джерела повідомлення («first originator») у межах Індії [324].

3. Кодекс етики та трирівнева система розгляду скарг: платформи, що публікують новинний або кураторський контент, підлягають цифровому кодексу етики. Особливістю документа є трирівнева система розгляду скарг, яка включає наступні рівні:

Рівень I: *саморегуляція видавця* (Grievance Redressal Officer). Кожна цифрова платформа, що підпадає під дію Кодексу, повинна призначити уповноважену особу (Grievance Officer), яка розглядатиме звернення громадян щодо можливих порушень. Цей офіцер зобов'язаний дати відповідь не пізніше ніж через 15 днів з моменту отримання скарги.

Рівень II: *апеляція до незалежного саморегулівного органу* (Self-Regulating Body). Якщо скаржник не задоволений відповіддю або її відсутністю, він може звернутися до зареєстрованого саморегулівного органу, очолюваного колишнім суддею Верховного чи Високого суду Індії. Такий орган має повноваження розглядати апеляції та видавати рекомендації платформам.

Рівень III: державний нагляд. Найвищий рівень контролю забезпечується урядом Індії через Inter-Departmental Committee (IDC) — міжвідомчий орган, який включає представників міністерств інформації та мовлення, електроніки та інформаційних технологій, юстиції тощо. IDC має право ухвалювати обов'язкові для виконання рішення, зокрема щодо вилучення або обмеження доступу до контенту, який порушує законодавство або моральні засади [324].

4. Автоматизоване фільтрування контенту:

Significant Social Media Intermediaries (SSMI) взяли зобов'язання впроваджувати ефективні механізми превентивного виявлення, модерації та видалення контенту, що становить загрозу суспільній безпеці та моральним засадам. Серед ключових інструментів – використання автоматизованих технологій фільтрації контенту, зокрема алгоритмів на основі штучного інтелекту (AI-based systems).

Згідно з правилами, платформи, які мають понад 5 мільйонів користувачів, зобов'язані впроваджувати програмні рішення, здатні:

- автоматично виявляти та блокувати вміст, що стосується сексуального насильства, дитячої експлуатації, тероризму або мови ворожнечі;

- здійснювати аналіз і класифікацію контенту за ступенем ризику поширення шкоди чи порушення прав людини;

- застосовувати людський контроль для перевірки автоматичних рішень (human-in-the-loop oversight), з метою уникнення алгоритмічної упередженості, порушення права на свободу висловлення думок або помилкового маркування контенту;

- проходити незалежний аудит точності та справедливості алгоритмів не рідше ніж раз на шість місяців [287].

Таким чином, автоматизовані системи розглядаються не як замінники, а як інструменти підтримки людських рішень у сфері модерації. Вони дозволяють оперативно реагувати на критичні ситуації, але не усувають потребу в етичному нагляді та правовому регулюванні.

У цілому, модель Індії забезпечує як горизонтальну, так і вертикальну інтеграцію механізмів контролю за онлайн-контентом, поєднуючи елементи саморегуляції, галузевого нагляду та державного втручання. Цей документ демонструє системний підхід до регулювання цифрової екосистеми – включно з міжвідомчою відповідальністю, прозорою політикою публікацій та структурою обов'язкової етики для великих платформ. Механізм вирішення скарг та встановлення офіцерів відповідальності забезпечує баланс між свободою висловлювань та захистом прав користувачів.

Узагальнюючи аналіз національних підходів до регулювання цифрової поведінки державних службовців, можна виділити низку спільних принципів і унікальних особливостей. Для наочності ключові елементи цих моделей подано у порівняльній таблиці, що дозволяє зіставити нормативні підходи, механізми реалізації та контекстні відмінності між країнами (табл. 3.1.). Такий

аналіз сприяє виявленню ефективних практик, які можуть бути адаптовані до українського адміністративного контексту.

Таблиця 3.1

Порівняльна таблиця міжнародного досвіду регулювання цифрової поведінки державних службовців

Країна	**Документ/ інструмент**	**Основні принципи**	**Механізми реалізації**	**Особливості**
Нідерланди	Code of Conduct for the use of Social Media by Civil Servants	Публічна відповідальність, політична нейтральність, лояльність, доброчесність, уникнення дискримінації та хейту	Обов'язкове ознайомлення; HR-семінари; гайдлайни; підтримка етичними кейсами	Регламент охоплює особисті акаунти і позаробочий час; вимагає уникнення критики керівництва; баланс між свободою і службовим статусом
Велика Британія	*Social Media Guidance for Civil Servants*, *SAFE Framework*, *Digital Communication Guidelines*	Об'єктивність, неупередженість, етичність, розмежування приватного/службового, оцінка ризиків	Офіційні гайдлайни від GCS; вбудовані етичні стандарти в урядову комунікацію; внутрішні інструкції комунікаційним підрозділам	Положення поширюються навіть на «приватні» повідомлення; застосовується до всіх службовців, особливо – до IT-команд
Канада	*Best Practices for Public Servants on Their Personal Use of Social Media*	Політична нейтральність, розмежування сфер, недопущення розголошення службової інформації, дотримання стандартів довіри	Рекомендаційний документ; персоналізовані кейси; вбудовані в кадрову політику	Зосередження на конфлікті інтересів; пояснення ризиків, пов'язаних із лайками, поширенням, коментарями – навіть із особистого акаунта
Естонія	Estonian Officials' Ethics Code; рекомендації Public Service Ethics Council; внутрішні політики цифрової комунікації міністерств; ініціативи NCSC-EE	Доброчесність, нейтральність, професійна лояльність, утримання від дискредитації органу влади, відповідальність у соцмережах	Загальні етичні норми в кодексі; рекомендації Ради з етики; обов'язок органів влади розробляти власні цифрові політики; тренінги та просвітницькі кампанії NCSC-EE	Відсутність спеціального цифрового кодексу; поведінка у соцмережах трактується як продовження публічної ролі; регулювання поєднує етичні принципи, інституційні політики та освітні ініціативи, забезпечуючи гнучкість без надмірного регуляторного тиску

Продовження табл. 3.1

Ірландія	*Civil Service Code of Standards and Behaviour*, Циркуляр 19/2009	Доброчесність, політична нейтральність, відповідальність, лояльність	Кодекс як умова працевлаштування; заборона політичної участі без дозволу; комунікаційне регулювання позаробочого часу	Заборонено публічно підтримувати чи критикувати політичні кампанії в соціальних мережах навіть у вільний від роботи час
Болгарія	*Кодекс поведінки державних службовців* (ПМС № 57, 2020)	Законність, лояльність, добросовісність, безсторонність, політична нейтральність, контроль емоцій	Нормативне закріплення; дисциплінарна відповідальність; розділ про цифрову поведінку	Указує на обов'язок уникати дій, що знижують престиж держслужби, включно з контентом у соцмережах поза межами роботи
Індія	*Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*	Етика цифрової поведінки, прозорість, відповідальність за контент, належна обачність, захист прав користувачів	Трирівнева система розгляду скарг: Grievance Officer – Self-Regulating Body – Inter-Departmental Committee; фільтрація AI	Вимагає призначення відповідальних осіб на платформах; автоматичний моніторинг контенту; обов'язковий аудит алгоритмів; сильна держрегуляція великих платформ

В Україні питання формування цифрових етичних стандартів у публічному секторі поки що не отримало належного інституційного оформлення. Водночас результати емпіричного дослідження, представлені в попередньому розділі, свідчать про наявність проблемних зон у цифровій поведінці державних службовців: від розмитих меж професійного/особистого в онлайновій комунікації – до високого рівня толерантності до агресії та прокрастинації в цифровому середовищі.

У цьому контексті доцільним є запровадження корпоративного цифрового етичного кодексу в системі державної служби України, що міг би включати:

- рекомендації щодо безпечної поведінки в соціальних мережах з урахуванням публічного статусу службовця;

- принципи толерантності, поваги та недискримінації в онлайн-комунікації, з урахуванням чутливих тем (гендер, релігія, політика, національність);
- заборону на публічне поширення службової інформації без погодження із керівництвом;
- протоколи реагування на випадки кібербулінгу й кіберхейту (з опорою на HR, IT-відділи, юристів та психологів);
- визначення стандартів цифрового персонального бренду державного службовця, як інструменту підвищення довіри громадськості до державної служби.

Ключовим завданням при імплементації такого кодексу є його інтеграція в систему навчання та підвищення кваліфікації. Так, у Канаді та Великобританії модулі з цифрової етики вже включені до стандартних освітніх програм CPD (Continuing Professional Development) для держслужбовців (Canada School of Public Service, 2022), а в Естонії розроблено державну платформу e-Governance Academy, яка пропонує онлайн-курси з цифрової доброчесності [296].

Варто зазначити, що міжнародна практика демонструє багатовекторність підходів до формування етичної поведінки держслужбовців у цифровому просторі. Узагальнений аналіз відповідних кодексів, інструкцій та стратегій у таких країнах, як Нідерланди, Велика Британія, Канада, Болгарія та Індія, дозволяє сформувати порівняльну матрицю (табл. 3.2.).

Виходячи з міжнародного досвіду та результатів емпіричного дослідження, представленого у розділі 2, в Україні доцільно запровадити поетапну модель цифрової етики в державній службі, орієнтуючись на успішні практики вище зазначених країн:

Таблиця 3.2.

Систематизовані рекомендації для України на основі досвіду п’яти країн

Країна	Ключові елементи досвіду	Рекомендації для України
Нідерланди	Спеціальний Кодекс поведінки для держслужбовців щодо соціальних мереж: – охоплює як робочий, так і позаробочий час; – регламентує навіть приватну активність у мережі; – забороняє публічну критику керівництва та участь у хейті; – підтримується навчальними програмами, гайдлайнами та щорічним оновленням.	– Розробити окремий цифровий кодекс для держслужбовців, що охоплює як службову, так і приватну онлайн-комунікацію; – Заборонити критику керівництва, політичні заяви, участь у хейті; – Підготувати адаптовані до України методичні матеріали; – Впровадити щорічне оновлення кодексу з урахуванням цифрових змін.
Канада	Документ *Best Practices for Public Servants on Their Personal Use of Social Media*: – політична нейтральність, професіоналізм і конфіденційність як основа цифрової поведінки; – чітке розмежування особистого і службового; – цифрова активність може впливати на довіру до інституції.	– Використати документ як зразок для формування українського регламенту поведінки у соцмережах; – Підкреслити баланс між свободою слова й нейтральністю; – Врахувати ризики гібридних загроз та цифрової політизації.
Велика Британія	*Social Media Guidance for Civil Servants + SAFE Framework + Digital Communication*: – регламентує поведінку навіть у «приватному» цифровому просторі; – забезпечує навчання, інституційний контроль та стандарти етики; – підкреслює відповідальність за особисту поведінку онлайн.	– Прийняти цифровий кодекс з урахуванням стандартів об’єктивності та відповідальності; – Імплементувати SAFE Framework (Separate, Assess, Factual, Ethical); – Розробити механізми реагування на порушення в цифровому середовищі; – Проводити системне навчання з цифрової доброчесності.
Естонія	*Estonian Officials' Ethics Code + рекомендації Public Service Ethics Council + внутрішні цифрові політики міністерств + ініціативи NCSC-EE:* – поведінка в соцмережах трактується як продовження публічної ролі; – етична відповідальність навіть при використанні приватних акаунтів; – усі органи влади зобов’язані мати власні політики цифрової комунікації; – просвітницькі та тренінгові програми з цифрової гігієни.	– Запровадити модель інтеграції етичних принципів у цифрову поведінку без окремого кодексу; – Розробити інституційні політики цифрової комунікації в усіх органах влади; – Поширити практику роз’яснень і рекомендацій від Ради з етики; – Використати національні просвітницькі ініціативи для підвищення цифрової культури держслужбовців.

Продовження табл. 3.2

Болгарія	*Кодекс поведінки держслужбовців* (2020): – містить окремі статті про цифрову поведінку; – охоплює службову та приватну онлайн-активність; – передбачає дисциплінарну відповідальність за порушення; – зобов'язує уникати конфліктів і некоректної поведінки у соцмережах.	– Інтегрувати положення про цифрову поведінку в Кодекс держслужбовця; – Чітко визначити межі дозволеної цифрової активності; – Встановити систему дисциплінарної відповідальності за порушення цифрових норм; – Поширити етичний контроль на позаробочий час.
Індія	*IT Rules 2021*: – зобов'язання для платформ (SSMI): офіцери відповідальності, системи скарг, AI-модерація; – кодекс етики для новинних і кураторських ресурсів; – три рівні розгляду скарг: саморегуляція, незалежне регулювання, міжвідомчий контроль.	– Розробити уніфіковану модель модерації контенту в держсекторі; – Визначити ризикові рівні цифрової комунікації держслужбовців; – Запровадити механізми саморегуляції та внутрішньої апеляції; – Упровадити технології AI-моніторингу з людським наглядом і захистом даних.

1. Розробка та впровадження «Кодексу цифрової поведінки державного службовця»:

- Включити до нього принципи етичної поведінки в інтернеті: службова нейтральність, лояльність, прозорість, недискримінація, повага до приватності, протидія кіберхейту, відповідальність за публічні висловлювання.
- Передбачити стандарти поведінки як у службовому, так і в особистому цифровому просторі (аналогічно до Великої Британії та Канади).
- Визначити обмеження публічного поширення службової інформації та участі в хейті.

2. Створення інституційного механізму реалізації:

- Призначення відповідальних посадових осіб у кадрових службах для моніторингу цифрової комунікації та консультацій з цифрової етики.
- Розробка внутрішніх механізмів розгляду скарг та консультацій для службовців, що зазнали кібербулінгу/дискримінації або будь-якого іншого виду онлайн-насильства.

- Використання SAFE-платформ або чек-листів для самоперевірки контенту перед публікацією.

3. Навчання, підвищення кваліфікації та просвітницька робота:

- Інтеграція модулів цифрової етики до програм підвищення кваліфікації державних службовців (зокрема, в програми Національного агентства з питань держслужби).
- Проведення регулярних тренінгів та інструктажів з юридичної та етичної відповідальності за публікації в мережі.
- Розробка інформаційних буклетів та інструкцій на основі кращих практик із прикладами типових порушень і правильних кейсів.

4. Адаптація до українських реалій:

- Врахувати результати опитування (див. розділ 2): високий рівень онлайн-прокрастинації, недостатній рівень довіри до керівництва, значна поширеність кіберхейту.
- Посилити механізми захисту службовців, які стали жертвами онлайн-насильства (кібербулінгу, кіберхейту, тощо).
- Забезпечити правове розмежування між приватною та службовою комунікацією.

Таким чином, впровадження корпоративного цифрового етичного кодексу в Україні з урахуванням кращих міжнародних практик не лише сприятиме безпечнішій і доброчесній поведінці службовців у мережі, але й стане дієвим інструментом формування нової цифрової культури державної служби в умовах кіберсоціального суспільства.

Також варто зазначити, що цифрові етичні кодекси повинні стати не лише формальними регламентами поведінки, а й дієвими інструментами формування професійної культури цифрового спілкування в публічному секторі. Їх запровадження в Україні сприятиме підвищенню довіри до державної служби, ефективнішій реалізації політики кібербезпеки та гармонізації міжособистісної взаємодії у кіберпросторі.

Зважаючи на кращі міжнародні практики досліджених країн, варто імплементувати такий інструмент для аналізу, прогнозування та трансформації поведінки державних службовців у цифровому середовищі як Агентно-базоване моделювання соціальних систем (Agent-Based Social Simulation, ABSS). Основна ідея цього підходу полягає у створенні моделей, які імітують взаємодію автономних агентів – умовних індивідів, що діють згідно з визначеними правилами в певному соціальному або організаційному контексті [300].

У контексті публічного управління агентно-базоване моделювання дозволяє не лише досліджувати індивідуальні реакції на управлінські інтервенції, але й враховувати такі критично важливі чинники, як:

- соціальні норми (дескриптивні та інжунктивні),
- впливи цифрового середовища (зокрема соціальні мережі),
- прояви хейту, поляризації чи дезінформації,
- внутрішньоколективні патерни спілкування.

Такі моделі дають змогу створювати експериментальні сценарії (наприклад, введення нових етичних кодексів цифрової поведінки) та оцінювати їхній потенційний вплив до моменту фактичного впровадження, знижуючи ризики адміністративних помилок або неефективності політик [291].

Застосування ABSS є особливо актуальним для оцінки ефективності цифрових етичних інтервенцій. Наприклад, у випадках, коли необхідно виявити, як змінюватиметься поведінка службовців у відповідь на введення обов’язкового дотримання соціальних норм у соцмережах, розмежування публічного/приватного профілю або запровадження тренінгів з цифрової доброчесності. Крім того, ABSS надає можливість:

– моделювати стратегії боротьби з онлайн-девіантною поведінкою, включаючи кібербулінг або витік службової інформації;

– розробляти адаптивні сценарії цифрової трансформації, ураховуючи культурні й організаційні особливості інституцій;

– створювати цифрових двійників державної установи – симуляційне середовище, в якому тестуються нові форми цифрової комунікації, взаємодії та контролю [225].

Наукові дослідження підтверджують, що ABSS-моделі є ефективним інструментом розробки соціальної політики в умовах складної поведінкової динаміки, особливо коли йдеться про вразливі соціальні механізми [233]. У публічному секторі це дає змогу зробити управління персоналом більш адаптивним, науково обґрунтованим і зорієнтованим на динамічні зміни в цифровій культурі.

Одним із практичних прикладів використання агентно-базованого моделювання (ABSS) у публічному управлінні є симуляційне дослідження, проведене у Великій Британії у співпраці з Behavioural Insights Team (BIT) та Центром урядової цифрової комунікації (Government Communication Service). Метою моделювання було передбачення змін у поведінці держслужбовців після запровадження оновлених настанов щодо цифрової етики – Social Media Guidance for Civil Servants [257].

Основні параметри моделі:

Агенти – державні службовці різних категорій (від молодших спеціалістів до керівників відділів), кожен із яких мав індивідуальні установки, рівень впливу колег та обізнаність про кодекс.

Середовище – умовна організація зі змінним цифровим контекстом (наприклад, публічний скандал, кампанія з дезінформації, тощо).

Інтервенції – введення тренінгів із цифрової етики, повідомлення з соціальними нормами, зміна санкційної політики за порушення кодексу.

У результаті симуляції протягом 12 місяців після впровадження моделі на 37% зросла ймовірність утримання від публікацій із політичним підтекстом; на 21% зменшився рівень цифрової неетичної поведінки (наприклад, лайків публікацій із кіберхейтом); підвищився коефіцієнт взаємного контролю колег, що сприяв посиленню норм самоцензури в межах професійної етики.

Моделювання дозволило протестувати кілька сценаріїв (наприклад, із та без тренінгів, або з різною жорсткістю норм), що допомогло уряду сформувати оптимальні стратегії впровадження етичного кодексу [222]. Як наслідок, результати були використані для підготовки оновлених програм підвищення кваліфікації для ІТ-фахівців у державних структурах.

Таким чином, використання агентно-базованого моделювання в контексті розробки та імплементації цифрових етичних кодексів для державних службовців постає не лише як інноваційний підхід, але й як науково вивірений метод підвищення ефективності та передбачуваності державної кадрової політики.

Загалом можна зробити висновок, що застосування соціальної інженерії як інструмента трансформації кадрової політики може включати такі практики:

- використання психологічних протоколів поведінки в онлайн-комунікації як частини службових інструкцій;
- регулярні тренінги з цифрової гігієни та стійкості до маніпуляцій, що базуються на аналізі кейсів соціотехнічних атак;
- імплементація етичних кодексів цифрової поведінки з урахуванням принципів soft governance;
- проведення ред-тімінгових симуляцій кіберзагроз [292] для підвищення готовності персоналу до психологічного тиску.

Таким чином, соціальна інженерія у позитивному ключі виступає важливим інструментом удосконалення кадрової політики, спрямованої на підвищення цифрової культури, психологічної стійкості та здатності державних службовців діяти конструктивно в умовах високої інформатизації.

3.2. Розвиток кіберпсихологічної компетентності державних службовців

Сучасна цифрова трансформація публічного управління супроводжується зростанням обсягів комунікацій у віртуальних середовищах, що, у свою чергу, вимагає від державних службовців не лише технічних знань, а й кіберпсихологічної компетентності. Кіберпсихологічна компетентність державного службовця у сучасних умовах цифровізації публічного управління розглядається як інтегративна характеристика особистості, що поєднує знання, уміння, навички та установки, які забезпечують безпечну, етичну та ефективну поведінку в кіберпросторі [273]. Її сутність полягає в здатності усвідомлювати психологічні особливості кіберпростору, прогнозувати наслідки цифрової поведінки, регулювати власні дії та протидіяти ризикам, включно з кібербулінгом, дезінформаційними впливами та емоційними перевантаженнями. Тобто, вона охоплює не лише технічні аспекти цифрової грамотності, а й психологічні, соціальні та етичні чинники взаємодії в мережевому середовищі [273].

У науковій літературі підкреслюється, що цифрове середовище формує специфічні виклики для публічної служби, пов’язані з інформаційними ризиками, онлайн-стресорами, віртуальною агресією та маніпулятивними технологіями впливу [217]. У цьому контексті кіберпсихологічна компетентність виконує функцію адаптивного ресурсу, що дозволяє державному службовцю не лише уникати кіберзагроз, але й діяти відповідно до етичних і професійних стандартів у цифрових комунікаціях [304].

Закордонні вчені виділяють різні компоненти в структурі кіберпсихологічної компетентності. Основними з них є:

Когнітивний – знання закономірностей онлайн-комунікації, цифрових ризиків, алгоритмічних упереджень і механізмів маніпуляції у віртуальних середовищах [273; 278].

Емоційно-регулятивний – здатність підтримувати психологічну стійкість під час цифрових конфліктів, хейту чи дезінформаційних атак [262; 284].

Етичний – дотримання принципів доброчесності, конфіденційності та недискримінації в онлайновій взаємодії [251].

Поведінковий – навички застосування етичних і безпечних моделей поведінки у кіберпросторі, дотримання корпоративних стандартів, своєчасного реагування на кіберінциденти та деструктивну поведінку [213] .

Мотиваційно-ціннісний – сформованість внутрішньої установки на дотримання принципів цифрової доброчесності, інформаційної відповідальності та професійної репутації у цифровому середовищі [211] .

Результати емпіричного дослідження, представленого у розділі 2, засвідчили, що рівень сформованості кіберпсихологічної компетентності в українських державних службовців є недостатнім. Зокрема:

- 77,7 % опитаних виявляють ознаки цифрової прокрастинації, що негативно впливає на продуктивність і підвищує ризик інформаційного перевантаження;
- лише 11,1 % респондентів регулярно звертаються по емоційну підтримку у випадку цифрових стресорів, що вказує на низький рівень емоційно-комунікативної готовності до роботи у кіберсередовищі;
- виявлено наявність професійних бар’єрів у повідомленні про кіберінциденти, зокрема страх негативної оцінки з боку керівництва;
- значна частка державних службовців демонструє недостатню цифрову саморегуляцію та низький рівень гігієни інформаційної взаємодії, що створює додаткові ризики у сфері кібербезпеки. Также аналіз емпіричних даних, отриманих у ході опитування державних службовців, дозволив виявити низку психологічних, поведінкових та організаційних вразливостей, що знижують ефективність їхньої діяльності у цифровому середовищі та створюють додаткові ризики для безпеки комунікацій. Виявлені проблемні зони можна згрупувати у п’ять основних блоків.

1. Цифрова прокрастинація та інформаційне перевантаження.

Понад три чверті респондентів (77,7 %) схильні відволікатися на несуттєві або другорядні онлайн-активності під час виконання службових обов'язків, що супроводжується підвищеною чутливістю до цифрових стимулів та збільшенням когнітивного навантаження. Це явище корелює з ефектом "attention residue" [281], коли залишкова увага після перемикання на сторонні завдання знижує продуктивність основної діяльності.

2. Недостатній рівень емоційно-комунікативної підтримки.

Лише 11,1 % опитаних заявили про регулярне звернення по емоційну підтримку у випадку цифрових стресорів, зокрема кібербулінгу чи токсичної комунікації. Відсутність налагоджених механізмів психологічної допомоги посилює ризики емоційного вигорання та знижує стресостійкість [285].

3. Бар'єри у повідомленні про кіберінциденти.

В опитуванні зафіксовано, що значна частина державних службовців не інформує керівництво або технічні підрозділи про виявлені цифрові загрози через страх отримати негативну оцінку. Подібні бар'єри комунікації знижують ефективність системи кіберзахисту і створюють "сліпі зони" у безпековому моніторингу [215].

4. Низький рівень цифрової саморегуляції та гігієни інформаційної взаємодії.

Респонденти продемонстрували недостатні навички контролю інформаційних потоків, що проявляється у зберіганні застарілих даних, некритичному поширенні неперевіреної інформації та недотриманні базових норм цифрової безпеки. Це підвищує вразливість до фішингових атак та маніпуляцій у соціальних мережах [331].

5. Толерантність до проявів кібербулінгу та кіберхейту.

За результатами опитування, частина держслужбовців демонструє пасивну позицію або навіть схвалення агресивних цифрових комунікацій, що створює передумови для нормалізації деструктивної поведінки в

організаційному середовищі. Така толерантність є несумісною з принципами цифрової етики та корпоративної культури [302].

Таким чином, ідентифіковані вразливості охоплюють як індивідуальний (психологічний, поведінковий), так і організаційний (комунікаційний, інституціональний) рівні, що вимагає комплексного підходу до їх подолання шляхом формування кіберпсихологічної компетентності та вдосконалення корпоративних стандартів цифрової поведінки.

Враховуючи все вищезазначене, кіберпсихологічну компетентність державного службовця доцільно структурувати за чотирма взаємопов'язаними компонентами (рис. 3.1.):

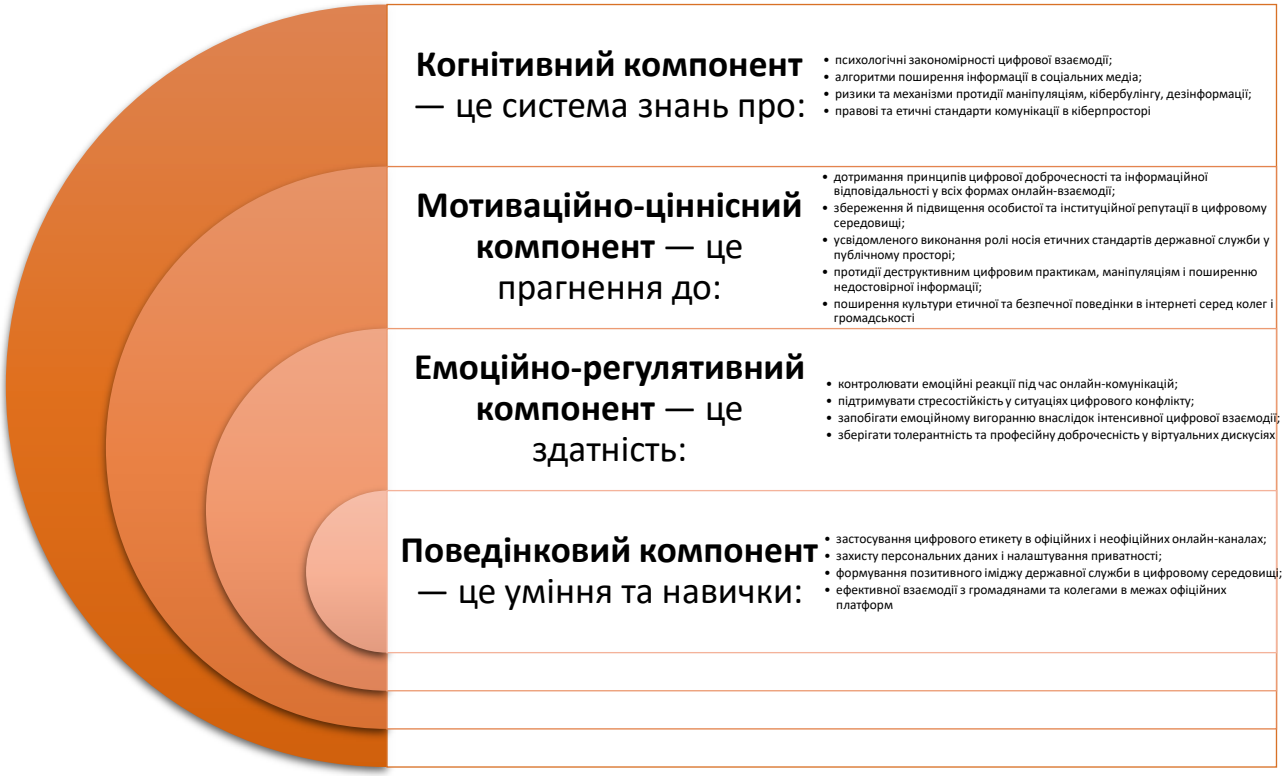

Рис. 3.1. Модель кіберпсихологічної компетентності державних службовців.

Когнітивний компонент передбачає формування у державних службовців системи знань про закономірності функціонування цифрового середовища, вплив онлайн-комунікацій на поведінку та психологічний стан, а

також про ризики, пов’язані з кіберзагрозами. Особливу увагу приділяють розумінню механізмів поширення інформації в соціальних мережах, ролі цифрових слідів, алгоритмів платформ і технологій маніпуляції.

Мотиваційно-ціннісний передбачає сформованість у державних службовців стійкої внутрішньої установки на дотримання принципів цифрової доброчесності, інформаційної відповідальності та підтримання високого рівня професійної репутації у цифровому середовищі. Він ґрунтується на усвідомленні ролі державного службовця як носія етичних стандартів у публічному просторі, розумінні довгострокових наслідків онлайн-поведінки для особистої та інституційної довіри, а також на готовності протидіяти деструктивним цифровим практикам, навіть за умови зовнішнього тиску чи спокус швидкого отримання популярності. Цей компонент стимулює не лише дотримання правил, а й активне просування культури етичної взаємодії в інтернеті серед колег та громадян.

Емоційно-регулятивний компонент визначає здатність державних службовців контролювати власні емоційні реакції у цифровому середовищі, зокрема під час конфліктних чи провокаційних комунікацій. Це включає розвиток стресостійкості, навичок уникнення емоційного вигорання, а також уміння підтримувати етичну поведінку навіть за умов кібербулінгу чи хейту.

Поведінковий компонент охоплює практичні навички безпечної та ефективної взаємодії в кіберпросторі, включно з умінням дотримуватися цифрового етикету, застосовувати захисні налаштування та технології безпеки, а також формувати позитивний імідж державної служби через особисту присутність у мережі. Цей компонент тісно пов'язаний із впровадженням корпоративних цифрових кодексів та дотриманням офіційних стандартів комунікації.

Таким чином, кіберпсихологічна компетентність виступає ключовим елементом сучасного професійного профілю державного службовця, що забезпечує інтеграцію психологічної стійкості, цифрової етики та комунікативної ефективності в умовах кіберпростору. Кіберпсихологічна

компетентність виступає ключовою передумовою ефективної роботи державних службовців у цифровому просторі, сприяє зниженню ризиків кіберзагроз і забезпечує гармонійне поєднання службових обов'язків із етичними нормами онлайн-взаємодії.

Важливим підґрунтям розвитку кіберпсихологічної компетентності є концепції digital emotional intelligence (EQ) та resilience training, що дозволяють формувати навички емоційної саморегуляції, виявлення прихованих загроз і конструктивного реагування на провокаційний контент [253].

Практичне впровадження таких компетенцій в системі державної служби передбачає:

1) включення модулів кіберпсихології до програм підвищення кваліфікації державних службовців, із фокусом на соціальні ефекти цифрових технологій, нейропсихологічний вплив контенту та методи самозахисту в інформаційних конфліктах;
2) розробку сценаріїв тренінгів з моделювання онлайн-ситуацій, що передбачають як позитивні, так і негативні комунікативні виклики, включаючи дезінформаційні вкиди, маніпулятивні меседжі, провокативні коментарі;
3) застосування інструментів симуляцій та ігрового навчання (serious games) для розвитку навичок адаптивної поведінки в умовах цифрових ризиків;
4) використання психологічних self-assessment інструментів, що дозволяють службовцям оцінити власний рівень готовності до конструктивної цифрової взаємодії.

Особливе значення має адаптація міжнародних практик до українських умов. Так, у Канаді, Великій Британії та Естонії цифрова етика і психологічна стійкість закріплені в системі Continuing Professional Development (CPD) та підтримуються внутрішніми тренінговими платформами [230; 329]. Досвід цих країн свідчить, що розвиток кіберпсихологічної компетентності сприяє підвищенню рівня довіри до державної служби, зниженню інцидентів

цифрових конфліктів та формуванню культури безпечного онлайн-спілкування.

В умовах гібридних загроз для України доцільним є поєднання підготовки з кібергігієни та психологічної грамотності в єдиній навчальній програмі, із застосуванням методів соціальної інженерії в етичному форматі для формування бажаних патернів цифрової поведінки. Це відповідає світовим трендам, де розвиток soft skills у кіберсередовищі визнається ключовим чинником ефективності державної служби [299].

Також, слід зауважити, що розвиток цифрового урядування та зростання ролі онлайн-комунікацій у діяльності публічної адміністрації зумовлює потребу у систематичному вимірюванні цифрово-поведінкової зрілості державних службовців. Під цим поняттям у сучасній науковій літературі розуміється інтегральний рівень сформованості цифрових компетентностей, емоційно-поведінкової стабільності та здатності дотримуватись етичних норм у кіберпросторі [247; 305]. Запровадження системи її вимірювання є ключовою передумовою цілеспрямованого розвитку кіберпсихологічної компетентності та адаптації кадрової політики до сучасних цифрових викликів.

Для комплексного оцінювання цифрово-поведінкової зрілості доцільно виділити структуру індикаторів цифрово-поведінкової зрілості, які складаються з трьох взаємопов’язаних блоків:

1. Технічна грамотність: рівень знань і навичок роботи з цифровими сервісами, дотримання протоколів кібербезпеки, здатність розпізнавати фішингові атаки та інші кіберзагрози.

2. Психологічна стійкість: здатність зберігати емоційну стабільність під час онлайн-взаємодії та інформаційного перевантаження; навички реагування на онлайн-критику або зіткнення з деструктивною поведінкою (наприклад, кібербулінгом чи хейтом), протидії маніпуляціям та психологічному тиску в цифровому середовищі, толерантність до стресових факторів. У міжнародній практиці для цього використовують шкали психологічної резильєнтності [234] та модифіковані опитувальники оцінки реакції на цифрові стресори [332].

3. Індикатори професійної відповідальності в мережі (комунікативно-етична складова): дотримання норм цифрового етикету, здатність вести конструктивний діалог у соціальних мережах, уникати конфлікту інтересів у публічних висловлюваннях, збереження політичної нейтральності, уникнення мови ворожнечі, а також уважне ставлення до поширення інформації. Ці показники можуть бути виміряні за допомогою поведінкових сценаріїв (behavioral vignettes) та аналізу рішень у симуляційних ситуаціях [288].

Запровадження таких індикаторів дає змогу не лише кількісно виміряти рівень зрілості, але й виявити профіль поведінкових ризиків у конкретного працівника чи структурного підрозділу.

Систематичний моніторинг рівня цифрово-поведінкової зрілості має поєднувати кілька методичних підходів:

– *регулярні анонімні опитування* – дозволяють виявляти суб'єктивне сприйняття цифрового робочого середовища, рівень стресу, задоволеність комунікаційною культурою та впевненість у власних цифрових навичках. Такі опитування рекомендовано проводити щонайменше двічі на рік, інтегруючи їх у внутрішні HR-процедури [299];

– *аналітика цифрової взаємодії* – з урахуванням вимог законодавства про захист персональних даних, можливо здійснювати аналіз метаданих внутрішніх комунікацій (наприклад, частоти використання корпоративних каналів, часу реакції на службові запити, частоти порушень комунікаційних протоколів);

– *симуляційні завдання (онлайн-квести) та навчальні тести* – формують уявлення про здатність службовця застосовувати етичні та безпечні практики у конкретних онлайн-ситуаціях, зокрема під час роботи з конфліктними коментарями, провокаційними запитами журналістів або фейковими інформаційними повідомленнями;

– *панельні дослідження* – застосовуються для відстеження динаміки цифрово-поведінкової зрілості одних і тих самих груп працівників протягом

тривалого періоду, що дозволяє оцінити ефективність інтервенцій (наприклад, тренінгів або впровадження цифрового етичного кодексу);

– метод «Peer review» – оцінка колегами проявів цифрової культури та командної взаємодії в онлайні.

Регулярність збору даних і порівнянність результатів у часі дадуть можливість не лише відслідковувати індивідуальний прогрес, але й змоделювати вплив організаційних змін на поведінку персоналу в кіберпросторі.

Для ефективної реалізації розвитку кіберпсихологічної компетентності даний моніторинг доцільно проводити щорічно, поєднуючи його з атестацією чи плановим підвищенням кваліфікації. Результати слід застосовувати для: індивідуалізації навчальних програм; визначення груп підвищеного ризику щодо кіберзагроз; оцінювання ефективності впроваджених етичних кодексів і цифрових політик.

Також у процесі оцінювання можна застосовувати цифрові аналітичні інструменти, наприклад:

✓ Digital Competence Framework (DigComp) Європейської комісії як базу для розробки локальних метрик. DigComp – це міжнародно визнаний фреймворк, розроблений Європейською комісією для стандартизації оцінки цифрових компетентностей [333]. Він описує ключові навички, знання та ставлення, необхідні для ефективної і безпечної роботи в цифровому середовищі. Цей фреймворк слугує базою для розробки локальних метрик, адаптованих під специфіку державної служби або організації. Тобто, можна виділити конкретні рівні володіння цифровими навичками (від початкового до експертного) і розробити тестові завдання, які відображають ці рівні. Наприклад, якщо на державній службі важлива здатність розпізнавати кіберзагрози, то за DigComp створюють тест, який оцінює розуміння фішингу, соціальної інженерії та інших атак.

✓ Behavioral Insights dashboards для візуалізації динаміки змін поведінкових показників. Behavioral Insights dashboards – це інтерактивні

інформаційні панелі, які візуалізують дані про поведінкові показники співробітників у цифровому середовищі. Вони допомагають аналізувати, як змінюється цифрова поведінка з часом, виявляти тенденції і проблемні зони. Дані збираються через опитування, аналітику комунікацій (наприклад, кількість відповідей на повідомлення, реакція на конфліктні ситуації), симуляції та інші методи. Потім ці дані відображаються у вигляді графіків, теплових карт або індикаторів прогресу. Наприклад, якщо у працівника зростає рівень стресу під час онлайн-взаємодії, це можна побачити на дашборді за допомогою опитувань та аналізу поведінки, що допоможе вчасно втрутитись. Приклад таких панелей можна побачити у дослідженнях Behavioral Insights Team (BIT) – провідної організації у сфері поведінкових наук.

✓ AI-модулі попереднього аналізу ризиків для виявлення потенційних зон поведінкової вразливості без втручання в приватну комунікацію. Це штучний інтелект, який автоматично аналізує великі обсяги цифрових даних співробітників (наприклад, метадані комунікацій, патерни поведінки) для виявлення потенційних зон поведінкової вразливості. AI-модулі працюють без втручання у приватний контент (не читають листи чи повідомлення), а аналізують структуру, частоту і тип взаємодій. Це дозволяє виявити ризики, наприклад, тенденції до конфліктної поведінки, перевантаження або недотримання цифрових протоколів. Наприклад, якщо співробітник різко змінює стиль спілкування або починає частіше ігнорувати повідомлення, AI-система може сигналізувати про можливі емоційні проблеми або втому. Подібні рішення впроваджуються в корпоративних цифрових платформах та системах кібербезпеки, наприклад, у Microsoft Viva Insights.

Слід зауважити, що вимірювання цифрово-поведінкової зрілості є не лише діагностичним, але й стратегічним інструментом управління персоналом у державному секторі, оскільки воно дозволяє: а) виявляти ключові вразливості та потреби у навчанні; б) прогнозувати ризики, пов’язані з

цифровою поведінкою; в) формувати адресні програми підвищення кваліфікації.

Таким чином, система моніторингу та вимірювання цифрово-поведінкової зрілості має стати інструментом не лише контролю, але й стратегічного розвитку персоналу. Її впровадження дозволить виявляти та оперативно усувати прогалини у компетентностях, а також забезпечувати адаптацію державної служби до швидких змін цифрового середовища. З цією метою, ми розробили Матрицю вимірювання кіберпсихологічної компетентності державних службовців (табл. 3.3.).

Таблиця 3.3.

Матриця вимірювання кіберпсихологічної компетентності державних службовців

Компонент кіберпсихологічної компетентності	**Ключові індикатори**	**Методи вимірювання**	**Інструменти оцінювання**
Когнітивний (система знань)	- Психологічні закономірності цифрової взаємодії - Алгоритми поширення інформації в соцмережах - Ризики та механізми протидії маніпуляціям, кібербулінгу, дезінформації - Правові та етичні стандарти комунікації в кіберпросторі	Стандартизовані тести; аналіз кейсів; тематичні сценарії	DigComp Framework; онлайн-тести (Moodle, Kahoot); сценарні завдання з виявлення ризиків і маніпуляцій
Мотиваційно-ціннісний (прагнення і цінності)	- Дотримання цифрової доброчесності та інформаційної відповідальності - Підвищення особистої та інституційної репутації - Усвідомлення ролі носія етичних стандартів державної служби - Протидія деструктивним практикам, маніпуляціям і дезінформації - Поширення культури етичної поведінки серед колег і громадськості	Аналіз рішень у етичних дилемах; самооцінка; опитування	Етичні кейс-тести; опитувальники моральних установок (Moral Foundations Questionnaire); поведінкові сценарії (behavioral vignettes)

Продовження табл. 3.3

Емоційно-регулятивний (контроль емоцій і стресостійкість)	- Контроль емоційних реакцій під час онлайн-комунікацій - Підтримка стресостійкості в цифрових конфліктах - Запобігання емоційному вигоранню - Толерантність і професійна доброчесність у віртуальних дискусіях	Психометричні опитувальники; кейс-симуляції; аналіз поведінки під стресом	Connor-Davidson Resilience Scale (CD-RISC); шкала емоційної регуляції (ERQ); модифіковані опитувальники цифрових стресорів
Поведінковий (цифровий етикет і взаємодія)	- Використання цифрового етикету в офіційних і неофіційних каналах - Захист персональних даних і налаштування приватності - Формування позитивного іміджу державної служби - Ефективна взаємодія з громадянами і колегами	Контент-аналіз; peer-review; аналіз цифрового профілю	Digital footprint analysis; шкала довіри в онлайн-середовищі; експертна оцінка HR; поведінкові симулятори
Інтегральний рівень цифрово-поведінкової зрілості	- Технічна грамотність: навички роботи з цифровими сервісами, розпізнавання кіберзагроз - Психологічна стійкість: емоційна стабільність, протидія маніпуляціям і кібербулінгу - Індикатори професійної відповідальності: цифровий етикет, політична нейтральність, уникнення мови ворожнечі	Комплексні індекси; панельні дослідження; аналіз цифрової взаємодії; симуляційні завдання	Digital Behavioural Maturity Index; Behavioral Insights dashboards; AI-модулі ризик-аналізу; онлайн-квести; peer review

Представлена матриця репрезентує авторську концепцію системного оцінювання кіберпсихологічної компетентності державних службовців, що ґрунтується на інтеграції когнітивних, мотиваційно-ціннісних, емоційно-регулятивних та поведінкових компонентів із комплексною оцінкою цифрово-поведінкової зрілості. Запропонована матриця поєднує змістовно-структурні характеристики компетентності (компоненти та їх ключові індикатори) із відповідними методами вимірювання та валідованими інструментами оцінювання, що дозволяє забезпечити надійність та об’єктивність діагностики.

Когнітивний компонент розглядається як система знань про психологічні закономірності цифрової взаємодії, алгоритми поширення інформації в соціальних медіа, ризики та механізми протидії маніпуляціям,

кібербулінгу та дезінформації, а також правові та етичні стандарти комунікації в кіберпросторі. Для його вимірювання пропонуються стандартизовані тести цифрової грамотності, сценарні завдання з виявлення ризиків та маніпуляцій, а також інструменти, адаптовані на основі Digital Competence Framework (DigComp) Європейської комісії.

Мотиваційно-ціннісний компонент відображає прагнення державного службовця до дотримання принципів цифрової доброчесності та інформаційної відповідальності, підтримання позитивної особистої та інституційної репутації, виконання ролі носія етичних стандартів державної служби, протидії деструктивним цифровим практикам та поширення культури етичної поведінки серед колег і громадськості. Оцінювання здійснюється шляхом аналізу рішень у змодельованих етичних дилемах, самооцінки етичної поведінки та використання етичних кейс-тестів і опитувальників моральних установок, зокрема Moral Foundations Questionnaire [260].

Емоційно-регулятивний компонент охоплює здатність контролювати емоційні реакції в онлайн-комунікаціях, підтримувати стресостійкість у ситуаціях цифрового конфлікту, запобігати емоційному вигоранню та зберігати професійну доброчесність у віртуальних дискусіях. Для вимірювання цього компонента застосовуються психометричні опитувальники, кейс-симуляції з емоційними тригерами, шкала психологічної резильєнтності Connor-Davidson Resilience Scale (CD-RISC) [234], шкала емоційної регуляції (Emotion Regulation Questionnaire, ERQ) [263] та модифіковані опитувальники оцінки реакцій на цифрові стресори [228].

Поведінковий компонент визначає уміння застосовувати цифровий етикет у різних каналах комунікації, захищати персональні дані, формувати позитивний імідж державної служби та здійснювати ефективну взаємодію в офіційних цифрових платформах. Для його оцінювання використовуються контент-аналіз цифрового профілю, метод «peer review», соціометричні опитування та інструменти аналізу цифрового сліду [252].

Інтегральний рівень цифровоповедінкової зрілості визначається шляхом комплексної оцінки трьох взаємопов'язаних блоків індикаторів: технічної грамотності, психологічної стійкості та професійної відповідальності в мережі. Для його вимірювання пропонуються комплексні індекси (Digital Behavioural Maturity Index), панельні дослідження, аналітика цифрової взаємодії, симуляційні завдання, а також сучасні цифрові аналітичні інструменти, зокрема Behavioral Insights dashboards для візуалізації динаміки змін поведінкових показників [318] та AI-модулі попереднього аналізу ризиків, що працюють без доступу до приватного контенту, але дозволяють виявляти патерни поведінкової вразливості [232].

Таким чином, представлена матриця є інструментом багатовимірного оцінювання кіберпсихологічної компетентності, що враховує не лише знаннєві й навичкові аспекти, але й емоційноціннісні та поведінкові характеристики, а також дозволяє здійснювати динамічний моніторинг рівня цифровоповедінкової зрілості з метою підвищення ефективності професійної діяльності державних службовців у цифровому середовищі.

Отже, зважаючи на те, що розвиток кіберпсихологічної компетентності державних службовців передбачає системну інтеграцію психологічних, поведінкових та технологічних знань у професійну підготовку та практичну діяльність персоналу, та враховуючи все вищезазначене, ми пропонуємо такі напрями формування кіберпсихологічної компетентності:

І. ***Впровадження регулярних тренінгів, воркшопів та онлайн-курсів з кіберпсихології та цифрової етики***. Рекомендується організовувати навчальні заходи з таких тематичних блоків:

- безпечна онлайн-комунікація та протидія цифровим загрозам;
- управління цифровим навантаженням і профілактика емоційного вигорання;
- алгоритми реагування на кібербулінг і кіберхейт у службовому та позаслужбовому контекстах;
- розвиток навичок критичного мислення та інформаційної гігієни.

Навчальні формати тут доцільно поєднувати: очні тренінги для командного опрацювання кейсів, онлайн-модулі для гнучкого доступу, симуляційні вправи з моделювання реальних інцидентів у кіберпросторі (за методами agent-based simulation).

II. ***Інтеграція теми кіберпсихологічної компетентності у систему підвищення кваліфікації та атестації державних службовців***. Пропонується закріпити у стандартах професійного розвитку вимогу проходження навчання з кіберпсихологічних аспектів щонайменше раз на два роки. Модулі мають охоплювати як теоретичну базу (зокрема, етичні норми, регламенти цифрової поведінки, принципи SAFE Framework), так і практичні навички, адаптовані до специфіки державної служби в умовах цифровізації. Доцільно передбачити оцінювання рівня засвоєння матеріалу за допомогою тестування та аналізу практичних кейсів.

III. ***Співпраця з психологами, медіаторами та фахівцями з кібербезпеки в межах кадрових підрозділів (HR-служб)***. Ефективне формування компетентності передбачає мультидисциплінарний підхід. Психологи можуть проводити діагностику рівня цифрового стресу та виявляти поведінкові ризики; медіатори — надавати підтримку у врегулюванні конфліктів, у тому числі в онлайн-середовищі; фахівці з кібербезпеки – консультувати щодо технічних аспектів захисту персональних та службових даних.

IV. ***Розробка корпоративних методичних матеріалів та інструкцій***. Доцільно створити єдиний пакет документів, який включатиме: цифровий етичний кодекс; довідники з реагування на кіберзагрози; візуальні схеми та чек-листи з інформаційної гігієни; алгоритми перевірки достовірності інформації.

Ці матеріали повинні бути доступні у внутрішніх інформаційних системах та оновлюватися щонайменше раз на рік.

V. ***Впровадження системи моніторингу та вимірювання цифрово-поведінкової зрілості персоналу***. Пропонується використовувати комплексні

індикатори, що охоплюють технічну, психологічну та комунікативну складові. Результати моніторингу слід застосовувати для індивідуалізації програм навчання та профілактики ризиків.

Таким чином, формування кіберпсихологічної компетентності має здійснюватися не як разова ініціатива, а як постійний процес, інтегрований у стратегію управління персоналом державної служби. Його реалізація сприятиме підвищенню цифрової безпеки, зниженню рівня кіберризиків та зміцненню професійної етики у кіберпросторі.

3.3. Пропедевтика кібербулінгу та кіберхейту в системі державної служби України

Розвиток кіберпсихологічної компетентності державних службовців, розглянутий у попередньому пункті, охоплює не лише формування навичок безпечної та етичної взаємодії у цифровому середовищі, але й здатність вчасно розпізнавати, запобігати та ефективно реагувати на прояви цифрової агресії. Серед форм такої агресії особливу увагу заслуговують кібербулінг та кіберхейт, які, згідно з результатами емпіричного дослідження представленими у розд. 2, мають як зовнішні (суспільно-політичні, медійні) так і внутрішні (організаційні, міжособистісні) детермінанти. Аналіз цифрової поведінки державних службовців свідчить про існування чотирьох основних форм прояву цифрової агресії:

1. Вербальні атаки у відкритих каналах комунікації: образливі коментарі, публічні звинувачення, дискримінаційні висловлювання у соціальних мережах або месенджерах.

2. Таргетований хейт: систематичне поширення негативного контенту щодо конкретної особи з метою дискредитації.

3. Кібербулінг у внутрішніх комунікаційних платформах: маніпулятивні повідомлення, приниження чи ігнорування у службових чатах, що призводить до психологічного тиску.

4. Поширення чуток та дезінформації: свідоме створення або передача неперевіреної інформації, що шкодить репутації колег або установи.

Виявлені джерела кіберхейту серед держслужбовців включають: особисті конфлікти, що переходять у цифрову площину; реактивну комунікацію у відповідь на стресові ситуації або управлінські рішення; поширення зовнішніх політичних і соціальних наративів у внутрішні комунікаційні канали; відсутність чітких регламентів цифрової етики.

Причини агресивної поведінки, за даними дослідження, найчастіше пов’язані з реактивними емоційними відповідями (імпульсивні реакції на коментарі або повідомлення), прагненням до помсти за реальні чи уявні образи, а також із низьким рівнем емоційної саморегуляції, зумовленим перевантаженням або поганим настроєм.

У сучасних умовах цифровізації публічного сектору кібербулінг та кіберхейт набувають системного характеру через особливості онлайн-комунікації – анонімність, асинхронність та швидке поширення інформації [277; 282]. Їхній вплив у державній службі є подвійно небезпечним: з одного боку, він порушує психологічний комфорт та професійне благополуччя службовців, з іншого – створює ризики репутаційних втрат для державних інституцій.

Так, кібербулінг у сфері державної служби, навіть у латентних або непрямих формах, має значний негативний вплив на ефективність функціонування кадрових систем та якість публічного управління. Згідно з дослідженнями Європейського агентства з безпеки та гігієни праці [245] та OECD [330], регулярний вплив цифрової агресії призводить до ряду системних наслідків:

По-перше, зниження індивідуальної та командної ефективності. Постійний психологічний тиск та деструктивна атмосфера в цифрових каналах комунікації сприяють відволіканню уваги від службових завдань, підвищують рівень помилок та знижують якість прийняття рішень [261].

По-друге, професійне вигорання. Хронічний стрес, викликаний онлайн-агресією, корелює зі збільшенням випадків емоційного виснаження та деперсоналізації серед державних службовців. Це особливо актуально в умовах гібридного та дистанційного форматів роботи, де цифрова взаємодія є основною формою комунікації [285].

По-третє, зниження рівня довіри в колективі. Поширення чуток, публічне приниження та агресивна риторика у внутрішніх мережах руйнують соціальний капітал організації. Згідно з концепцією «психологічного контракту» [313], подібні інциденти знижують готовність працівників до співпраці та взаємної підтримки, що негативно впливає на колективну згуртованість.

По-четверте, репутаційні ризики для інституції. Кейсів, коли конфлікти у внутрішньому цифровому просторі ставали публічними, дедалі більше. Це шкодить іміджу державної служби, знижує рівень громадської довіри та може впливати на легітимність управлінських рішень [248].

Узагальнено результати наукових досліджень щодо наслідків кібербулінгу та кіберхейту в системі державної служби можна представити у вигляді схеми (рис. 3.2.).

Так, на індивідуальному рівні, як свідчать дослідження, тривала цифрова агресія призводить до хронічного стресу, емоційного виснаження та зниження продуктивності.

На командному рівні у колективах спостерігається зниження рівня довіри, порушення внутрішньої комунікації та зростання конфліктності, що прямо впливає на ефективність роботи.

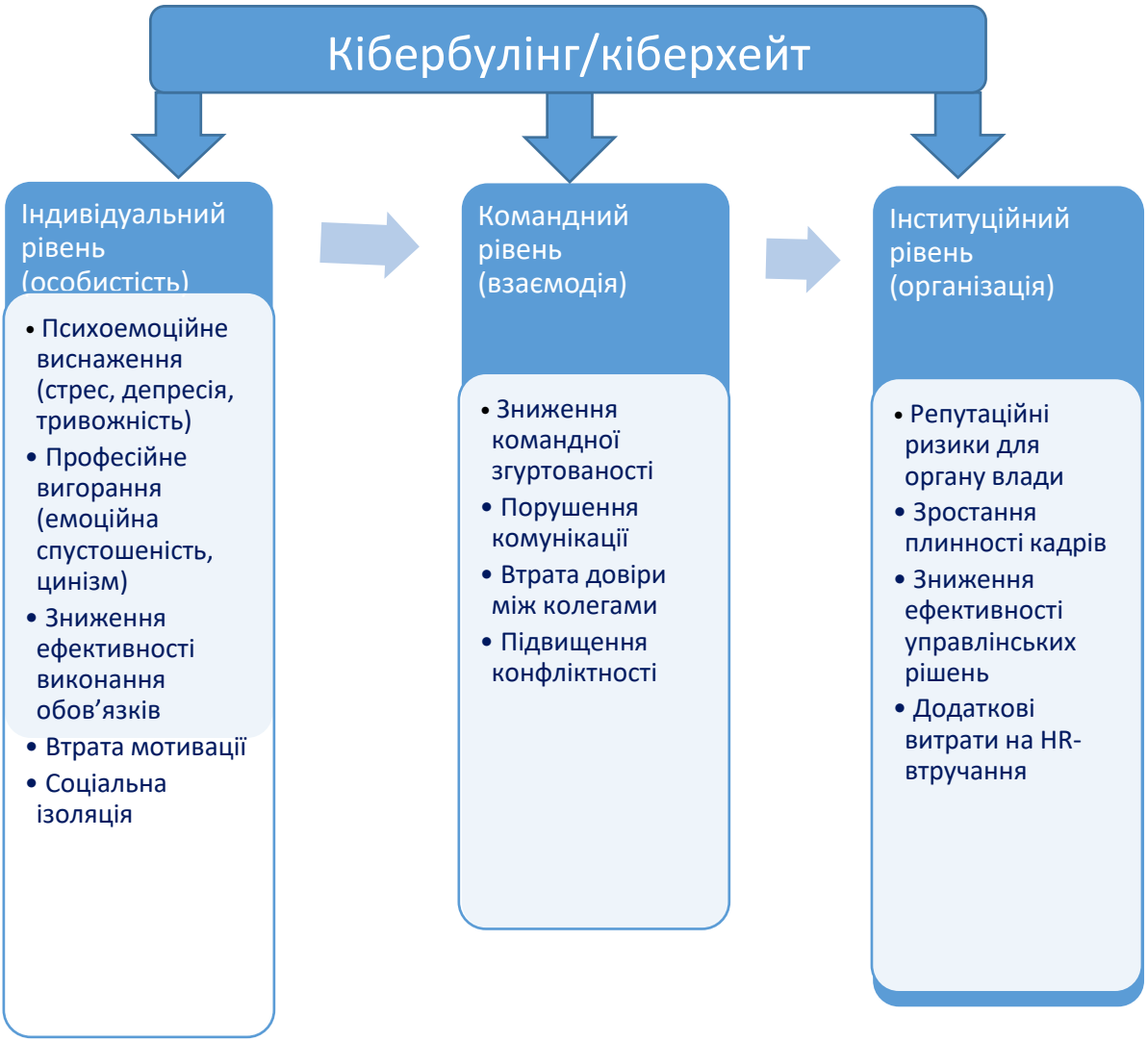

Рис. 3.2. Наслідки кібербулінгу в професійному середовищі

На інституційному рівні випадки кібербулінгу та кіберхейту можуть призводити до втрати репутації державних органів, збільшення плинності кадрів та додаткових витрат на кризове управління і кадрову підтримку.

Отже, кібербулінг та кіберхейт в професійному середовищі не є лише міжособистісною проблемою, а виступають як фактори, що підривають організаційну ефективність, кадрову стабільність і суспільну довіру до державного сектору. Їх превенція та нейтралізація повинні розглядатися як складова системної політики управління персоналом у вимірах кіберпростору.

Таким чином, перехід від загальної концепції кіберпсихологічної компетентності до спеціалізованої пропедевтики кібербулінгу та кіберхейту є закономірним етапом формування цілісної системи управління людськими ресурсами у цифровому середовищі. Зазначений підхід базується на

принципах проактивного управління поведінковими ризиками та передбачає інтеграцію механізмів системного попередження деструктивних онлайн-практик шляхом поєднання трьох взаємопов'язаних блоків: превентивної освіти, інституційних процедур реагування та розвитку корпоративної культури нульової толерантності до цифрової агресії [248; 330].

Пропедевтика у цьому контексті визначається як система комплексних превентивних заходів, спрямованих на мінімізацію ризиків виникнення та ескалації кібербулінгу й кіберхейту, а також на підвищення стійкості державних службовців до цифрових стресорів. Вона повинна передбачати:

– розробку та впровадження внутрішніх протоколів реагування на випадки кібербулінгу та кіберхейту, що включають алгоритми повідомлення про інциденти, процедури конфіденційного розгляду та надання психологічної і юридичної підтримки постраждалим;

– інтеграцію навчальних модулів з емоційної саморегуляції, цифрової етики та інформаційної безпеки у програми підвищення кваліфікації, що безпосередньо корелюють з індикаторами емоційно-регулятивного та когнітивного компонентів (див. табл. 3.3.), вимірюваних за допомогою психометричних опитувальників (Connor-Davidson Resilience Scale, ERQ) та стандартизованих тестів цифрової грамотності;

– встановлення чітких стандартів онлайн-комунікації у внутрішньому регламенті установи з обов'язковим ознайомленням кожного державного службовця та регулярним тестуванням знань цих стандартів. Цей пункт напряму пов'язаний з індикаторами мотиваційно-ціннісного та поведінкового компонентів, що оцінюються через аналіз рішень у змодельованих етичних дилемах, поведінкові сценарії та метод «peer review»;

– створення спеціалізованих психологічних і медіаційних сервісів у складі HR-підрозділів для оперативного реагування, проведення профілактичних консультацій та посередництва у випадках цифрових конфліктів, з подальшим моніторингом результативності за допомогою комплексних індексів цифровоповедінкової зрілості (Digital Behavioural

Maturity Index) та аналітичних інструментів (Behavioral Insights dashboards, AI-модулі попереднього аналізу ризиків).

Таким чином, запропонована пропедевтична модель є не лише концептуальною рамкою для формування культури безпечної взаємодії у кіберпросторі, але й логічним підґрунтям для впровадження багатовимірного інструментарію оцінювання, поданого у табл. 3.3. Така інтеграція дає змогу поєднати превентивні заходи з постійним моніторингом ключових індикаторів – від когнітивної обізнаності та емоційної стабільності до етичної відповідальності й практик цифрового етикету – забезпечуючи, таким чином, цілісний цикл управління поведінковими ризиками у державній службі.

Зважаючи на викладені вище принципи пропедевтики кібербулінгу та кіберхейту, ключовим етапом у побудові системи кіберпсихологічної компетентності є конкретизація потенційних загроз, що можуть виникати у цифровому середовищі державної служби, та визначення цільових превентивних заходів. Як свідчить аналіз досвіду міжнародних організацій та національних досліджень, ефективність превентивних стратегій значно зростає, коли вони спираються на: чітку класифікацію форм цифрової агресії; оцінку ймовірних наслідків; формування алгоритмів реагування, інтегрованих у систему розвитку кіберпсихологічної компетентності.

Матриця компонентів та індикаторів, представлена у попередньому розділі, виконує роль концептуальної основи, де кожен ризик цифрової агресії може бути співвіднесений із певним компонентом та вимірюваний за допомогою індикаторів цифрово-поведінкової зрілості:

Вербальні атаки у відкритих каналах комунікації пов’язані з мотиваційно-ціннісним компонентом (дотримання етичних норм онлайн-взаємодії) та індикаторами професійної відповідальності в мережі.

Таргетований хейт відноситься до емоційно-регулятивного компоненту (стресостійкість, здатність уникати ескалації) і психологічної стійкості як блоку індикаторів.

Кібербулінг у внутрішніх платформах вимагає розвитку поведінкового компоненту (ефективна командна взаємодія, використання цифрового етикету) та індикаторів технічної грамотності для налаштування захисту і блокування агресорів.

Поширення чуток та дезінформації пов'язане з когнітивним компонентом (знання алгоритмів поширення інформації, факт-чекінг) та індикаторами технічної грамотності.

Реактивна комунікація у стресових ситуаціях стосується емоційно-регулятивного компоненту (контроль емоційних реакцій) і психологічної стійкості.

Зовнішні політичні/соціальні наративи у внутрішніх каналах зачіпають мотиваційно-ціннісний компонент (збереження нейтральності, уникнення конфлікту інтересів) та індикатори професійної відповідальності.

Відсутність чітких регламентів цифрової етики підпадає під когнітивний компонент (знання стандартів комунікації) та поведінковий компонент (послідовне дотримання цих стандартів).

Узагальнена систематизація таких ризиків і превентивних заходів, побудована з урахуванням цих зв'язків, подана у табл. 3.4, що дозволяє здійснити цільове планування освітніх, організаційних та нормативних інтервенцій у межах державної служби.

Таким чином, системна пропедевтика кібербулінгу та кіберхейту у державній службі України має ґрунтуватися на поєднанні організаційних регламентів, психологічної підтримки та розвитку кіберпсихологічної компетентності службовців, що дозволить знизити рівень цифрової агресії та підвищити якість комунікації у кіберпросторі.

Таблиця 3.4.

Основні ризики цифрової агресії в системі державної служби України та відповідні превентивні заходи

Форма / джерело ризику	Опис прояву	Можливі наслідки	Превентивні заходи
Вербальні атаки у відкритих каналах комунікації	Образливі коментарі, публічні звинувачення, дискримінаційні висловлювання у соцмережах та месенджерах	Погіршення психологічного клімату, зниження довіри до інституції	Запровадження етичного кодексу онлайн-комунікацій; регулярні тренінги з цифрової етики
Таргетований хейт	Систематичне поширення негативного контенту щодо конкретної особи	Репутаційні втрати, психологічний тиск, зниження мотивації	Протокол внутрішнього розслідування; медіаційна підтримка; алгоритми блокування та фіксації інцидентів
Кібербулінг у внутрішніх платформах	Маніпулятивні повідомлення, приниження чи ігнорування у службових чатах	Зниження командної ефективності, підвищення плинності кадрів	Створення HR-гарячої лінії; анонімні канали повідомлення; контроль внутрішньої комунікації
Поширення чуток та дезінформації	Створення/передача неперевіреної інформації, що шкодить репутації колег чи установи	Дестабілізація колективу, втрата довіри до керівництва	Верифікаційні протоколи; навчання факт-чекінгу; інформаційні бюлетені з роз’ясненнями
Реактивна комунікація у стресових ситуаціях	Імпульсивні емоційні відповіді без належної перевірки інформації	Ескалація конфліктів, порушення етичних норм	Навчання емоційній саморегуляції; впровадження «cool-down» періодів перед відправкою повідомлень
Зовнішні політичні/соціальні наративи у внутрішніх каналах	Перенесення політичних дискусій у робочі чати	Поляризація колективу, підрив нейтральності держслужби	Розмежування приватної та професійної комунікації; модерація внутрішніх каналів
Відсутність чітких регламентів цифрової етики	Невизначеність у правилах поведінки в мережі	Зростання ризиків цифрової агресії	Розробка та впровадження внутрішнього кодексу цифрової поведінки; щорічне оновлення документа

Також ефективна протидія кібербулінгу та кіберхейту в системі державної служби передбачає поєднання превентивних заходів і розбудову дієвих інституційних механізмів реагування. Міжнародний досвід свідчить, що лише інтегрований підхід, який поєднує нормативне врегулювання, внутрішні процедури, кадрову підтримку та моніторинг цифрової взаємодії, здатний забезпечити сталий ефект [244; 297]. Це передбачає роботу в таких напрямках:

1. ***Створення чітких внутрішніх регламентів і протоколів***. Необхідно розробити та затвердити уніфіковані Протоколи реагування на випадки цифрової агресії, які мають передбачати:

– визначення термінів кібербулінг, кіберхейт, цифрова агресія відповідно до чинного законодавства та внутрішніх політик;

– алгоритм дій для службовців, які зазнали або стали свідками агресії (зокрема, процедури фіксації інциденту, звернення до уповноважених осіб, конфіденційного розгляду скарг);

– чіткі строки розгляду випадків та порядок інформування постраждалих про результати;

– систему санкцій або дисциплінарних заходів для порушників, узгоджену з трудовим законодавством та етичним кодексом державної служби.

Важливо, щоб ці регламенти були публічно доступними всім працівникам та регулярно оновлювалися з урахуванням змін у цифровому середовищі.

2. ***Наявність відповідального підрозділу або посади в HR-департаментах***. У структурі кадрових служб (HR-департаментів) доцільно створити Сектор цифрової етики та безпеки комунікацій, який би:

– координував превентивні заходи, включно з навчальними програмами з кіберетики та кіберпсихологічної грамотності;

– приймав та обробляв звернення щодо випадків цифрової агресії;

– здійснював первинну психологічну підтримку або перенаправляв до кваліфікованих фахівців (психологів, медіаторів);

– вів анонімну статистику інцидентів для подальшого аналізу та звітування керівництву;

– забезпечував взаємодію з ІТ-відділом для збереження цифрових доказів і технічного блокування каналів агресії.

Запровадження такої посади, як цифровий омбудсмен або офіцер з цифрової етики, може підвищити довіру працівників до механізмів захисту та зменшити рівень латентності інцидентів.

3. ***Інтеграція у систему управління персоналом***. Запобігання кібербулінгу має бути інтегроване у комплексну стратегію управління персоналом, включаючи:

– обов’язкове ознайомлення нових працівників із цифровим етичним кодексом;

– включення модулів з кіберетики та управління конфліктами до програм підвищення кваліфікації;

– проведення регулярних тренінгів і симуляцій кризових комунікацій;

– моніторинг цифрового середовища за допомогою спеціалізованих ІТ-інструментів (з дотриманням норм конфіденційності).

Для унаочнення пропонується відповідна модель інституційної системи реагування на кібербулінг у державній службі (рис. 3.3).

Запропонована модель ґрунтується на принципах багаторівневої взаємодії між кадровими службами (HR), ІТ-підрозділами, керівництвом органу влади та службами психологічної підтримки. Її ключова мета – створити комплексний, скоординований і прозорий механізм протидії цифровій агресії, що поєднує оперативне реагування, психологічну реабілітацію та превентивну просвіту.

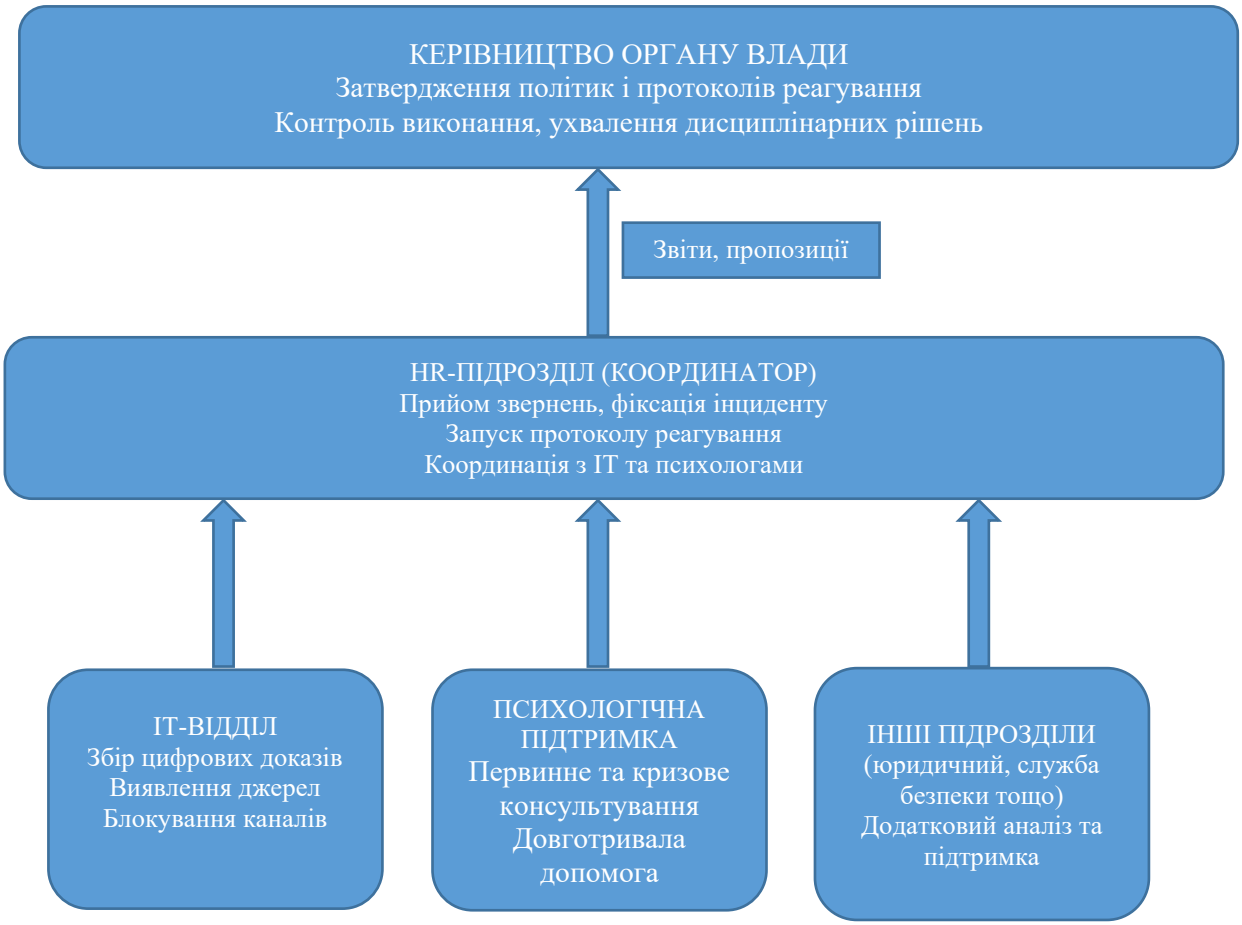

Рис. 3.3. Модель інституційної системи реагування на кібербулінг у державній службі України

Модель передбачає, що HR-підрозділ виступає головним координатором процесу, приймаючи первинні звернення, організовуючи розгляд інциденту, забезпечуючи конфіденційність та взаємодію із задіяними підрозділами. IT-відділ відповідає за збереження цифрових доказів, виявлення джерел агресії та технічне блокування каналів комунікації з порушником. Керівництво ухвалює управлінські рішення щодо дисциплінарних заходів і затверджує протоколи реагування, а також здійснює контроль за їх виконанням. Психологічна служба забезпечує постраждалим підтримку, у тому числі кризове консультування та довготривалу терапію у випадках глибокого стресового впливу.

Важливим елементом є зворотний зв’язок між підрозділами, що дозволяє вдосконалювати процедури реагування, а також впроваджувати

превентивні програми (тренінги з кіберетики, симуляційні навчання з кризових комунікацій, психологічні семінари) у систему підвищення кваліфікації держслужбовців.

Ключовими етапами роботи моделі є:

- ✓ Фіксація інциденту: службовець повідомляє про випадок кібербулінгу або кіберхейту до HR.
- ✓ Первинна оцінка: HR перевіряє обставини, координує збір доказів через ІТ-відділ.
- ✓ Психологічна підтримка: постраждалий отримує первинну консультацію.
- ✓ Адміністративні дії: керівництво ухвалює рішення про санкції або інші заходи.
- ✓ Превенція: впровадження навчальних програм, оновлення протоколів.

Таким чином, запропонована модель створює цілісний механізм реагування на кібербулінг і кіберхейт, у якому поєднано оперативне опрацювання інцидентів, технічний та психологічний супровід постраждалих і системну превенцію. Її багаторівнева структура забезпечує не лише ефективне вирішення окремих випадків, але й формування стійкої організаційної спроможності до протидії цифровій агресії.

Логічним наступним кроком у розвитку цієї системи є запровадження культури нульової толерантності до кібербулінгу та кіберхейту, формування якої потребує комплексного, системно організованого підходу, який буде включати як інформування та просвіту, так і створення реальних інституційних каналів підтримки. Міжнародні дослідження свідчать, що такі кампанії ефективні лише за умови, якщо вони поєднують постійний інформаційний вплив, залучення персоналу та наявність безпечних інструментів повідомлення [246; 276]. Це передбачає такі напрямки роботи:

1. ***Освітні заходи***. Рекомендується систематичне проведення тематичних семінарів, вебінарів та тренінгів, присвячених: розпізнаванню

ознак цифрової агресії; методам конструктивного вирішення конфліктів в онлайн-середовищі; практикам психологічної саморегуляції та управління емоціями.

Ці заходи мають інтегруватися в програми підвищення кваліфікації державних службовців (CPD) та включати як теоретичні модулі, так і практичні симуляції ситуацій. Згідно з OECD [297], включення елементів рольових ігор та моделювання реальних кейсів значно підвищує здатність службовців до своєчасного реагування на кіберзагрози.

2. ***Аналітичні звіти та платформи довіри***. Регулярна публікація узагальнених анонімізованих звітів про випадки цифрової агресії у відомстві формує атмосферу прозорості та стимулює керівництво до превентивних дій. Створення платформи довіри – онлайн-простору, де працівники можуть отримати консультації, ознайомитися з етичним кодексом, протоколами реагування та матеріалами з цифрової безпеки – дозволяє підвищити рівень поінформованості та знизити рівень латентності інцидентів.

3. ***Внутрішні інструменти повідомлення.*** Ефективне реагування можливе лише за наявності зручних і безпечних каналів інформування про інциденти кібербулінгу та кіберхейту, таких як: гарячі лінії, доступні в робочий і позаробочий час; чат-боти, які автоматично збирають інформацію про інцидент і надають подальші інструкції; анонімні онлайн-форми, що гарантують конфіденційність і захист персональних даних.

У міжнародній практиці ефективність таких інструментів зростає, якщо вони супроводжуються зрозумілою інструкцією, як і кому повідомляти про агресію, та забезпечують швидкий зворотний зв’язок.

Також було б доречним: а) запровадити щорічні внутрішні кампанії у форматі «Тиждень цифрової етики» з інтерактивними сесіями, конкурсами та залученням експертів; б) використовувати візуальні нагадування (плакати, скрінсейвери, інфографіку) про ключові принципи етичної взаємодії в кіберпросторі; в) інтегрувати тему цифрової доброчесності у корпоративні комунікації, зокрема, внутрішні бюлетені та офіційні онлайн-канали.

Враховуючи вищезазначене, доцільно представити модель комунікаційної кампанії нульової толерантності до кібербулінгу та кіберхейту для системи державної служби України (рис. 3.4.).

Рис. 3.4. Модель комунікаційної кампанії нульової толерантності до кібербулінгу та кіберхейту для системи державної служби України

Запропонована модель комунікаційної кампанії нульової толерантності ґрунтується на інтегрованому підході, який поєднує просвітницькі заходи, прозоре інформування та ефективні канали повідомлення про інциденти. Її структура передбачає тісну координацію між керівництвом, HR-відділами, IT-підрозділами та психологічними службами.

Перший блок – освітні заходи – забезпечує підвищення рівня цифрової грамотності та кіберпсихологічної стійкості персоналу шляхом впровадження

тренінгів, модулів у системі підвищення кваліфікації та практичних симуляцій.

Другий блок – аналітичні звіти та платформи довіри – формує атмосферу прозорості через публікацію узагальнених даних про випадки цифрової агресії та створення внутрішнього онлайн-простору з ресурсами для підтримки працівників.

Третій блок – інструменти повідомлення – передбачає наявність різноманітних безпечних і зручних каналів інформування про інциденти (гарячі лінії, чат-боти, анонімні форми), що дозволяє зменшити латентність проблеми.

Четвертий блок – додаткові активності – спрямований на підтримку постійного інтересу та залучення працівників через кампанії, візуальні нагадування та інформаційні матеріали, що створюють сталі поведінкові патерни нульової толерантності.

Взаємодія цих блоків забезпечує не лише оперативне реагування на випадки цифрової агресії, але й довгострокове формування корпоративної культури, орієнтованої на етичну, безпечну та психологічно комфортну комунікацію в кіберпросторі.

Висновки до 3 розділу

У ході аналізу та розробки рекомендацій враховано результати емпіричного дослідження (розд. 2), міжнародні стандарти цифрової етики та кращі управлінські практики. Так, представлено адаптовану модель імплементації кращих міжнародних практик щодо взаємодії державних службовців у кіберпросторі. Виокремлено успішні підходи Нідерландів, Великої Британії, Канади, Болгарії, Індії, Естонії, а також досвід Сінгапуру та Данії, де механізми «м’якого підштовхування» реалізуються через тонкі інтервенції у формі самопідказок у цифровому та організаційному просторах, використанні соціальних норм як підсилювачів відповідальності, а також

застосуванні сенсорних сигналів (колір, структура документа), що підвищують ймовірність позитивної поведінкової реакції. Ефективність таких інтервенцій підтверджується результатами рандомізованих контрольованих експериментів (RCT), що дозволяють кількісно вимірювати поведінкові зміни, пов'язані із запровадженням конкретних інформаційних форматів або повідомлень.

Логічним продовженням імплементації міжнародного досвіду став розвиток кіберпсихологічної компетентності державних службовців як ключової умови підвищення їхньої цифровоповедінкової зрілості. Визначено її структуру (когнітивний, емоційнорегулятивний, поведінковий, етичний компоненти), проаналізовано виявлені вразливості (низька стресостійкість, схильність до реактивної агресії, відсутність навичок протидії кібербулінгу). Запропоновано поетапну систему формування цієї компетентності через навчальні модулі, роботу HR-психологів, інтерактивні симуляції та моніторинг показників цифрової поведінки. Розроблено матрицю індикаторів для оцінювання рівня компетентності, що поєднує кількісні та якісні методи. Вимірювання цифрово-поведінкової зрілості інтегрується у кадрову політику як інструмент забезпечення безпечного, етичного та психологічно стійкого цифрового середовища.

Розкрито пропедевтику кібербулінгу та кіберхейту як складову цифрової безпеки кадрової політики. Визначено основні форми цифрової агресії, причини її поширення у держсекторі та проаналізовано ризики для ефективності роботи колективу (зниження довіри, вигорання, деструкція комунікаційних зв'язків). Запропоновано науково обґрунтовані моделі інституційних механізмів реагування, що передбачають створення протоколів дій, відповідальних HR-підрозділів, цифрових омбудсменів, а також реалізацію комунікаційних кампаній нульової толерантності до цифрової агресії з використанням освітніх платформ, чат-ботів та анонімних форм повідомлення.

Загалом, реалізація запропонованих заходів забезпечить інтеграцію цифрової етики та кіберпсихологічної грамотності у систему управління персоналом, сприятиме підвищенню стійкості державної служби до кіберзагроз, зміцнить довіру суспільства до публічної адміністрації та підвищить ефективність міжособистісної взаємодії у кіберпросторі.

ВИСНОВКИ

У дисертаційній роботі розв'язано актуальну проблему, яка полягає у науковому обґрунтуванні та розробці практичних рекомендацій щодо підвищення ефективності управління персоналом на державній службі у вимірах взаємодії в кіберпросторі. Одержані під час дослідження результати, а також реалізовані мета і завдання дозволяють зробити такі основні висновки:

1. Комплексний аналіз наукової літератури, нормативно-правових документів з теми дисертації довів, що не існує єдиної, цілісної і всеохоплюючої теорії, яка пояснювала б усі аспекти управління персоналом на державній службі у вимірах взаємодії в кіберпросторі. Під кіберпростором розуміється простір, обумовлений функціонуванням продуктів інформаційно-комунікаційних технологій, що дозволяють створювати складні системи взаємодій агентів (суб'єкти взаємодії) з метою отримання інформації, обміном та управління нею, а також здійснення комунікацій в умовах великої кількості мереж.

Доведено, що кіберпростір має трьохвимірну структуру, складовими якої є фізичні, інформаційні та соціальні компоненти. Особливості взаємодії в кіберпросторі обумовлені феноменами «кіберпсихологічна готовність», «кібербезпека», «кіберзахист», «кібергігієна».

Констатовано, що ризики в кіберпросторі охоплюють широкий спектр загроз як для організації (фінансові збитки, порушення конфіденційності даних, втрати репутації тощо), так і окремих осіб (порушення психічного здоров'я, професійне вигорання і т. ін.). Управління ризиками взаємодії в кіберпросторі повинна стани стрижнем HR-стратегій органів публічної влади.

2. Встановлено базові механізмами взаємодії державних службовців у кіберпросторі, а саме: організаційно-правовий, інформаційно-технічний, соціально-психологічний. Саме через призму розуміння функціонування цих механізмів можна оцінювати ефективність взаємодії державних службовців у

кіберпросторі, а також удосконалювати/модернізувати таку взаємодію, під впливом зовнішніх та внутрішніх факторів.

Основними передумовами парадигмальних зсувів в управлінні персоналом на державній службі є: цифровізація державного сектору; корпоративна та особиста кібербезпека державних службовців; взаємодія масмедіа та державної влади. Саме вони генерують необхідність впровадження комплексних змін у систему державної служби України, зокрема:

– обґрунтування концептуальних засад професійної діяльності державних службовців у кіберпросторі;

– впровадження нової компетентнісної моделі професійної діяльності державних службовців у кіберпросторі;

– модернізація технологій оцінювання готовності кандидатів на зайняття посад державної служби до здійснення професійної діяльності в умовах цифрового урядування та розвитку інформаційного суспільства;

– формування уявлень, цінностей і переконань про те, що цифрова компетентність, професійна мобільність, корпоративна та особиста кібербезпека стають стрижнем кар’єрного розвитку державних службовців.

3. Визначено стан готовності державних службовців до професійної діяльності в кіберпросторі. Встановлено, що професійна активність державних службовців у цифровому середовищі супроводжується як новими можливостями для ефективної комунікації, так і зростанням соціальних ризиків, насамперед – кіберзалякуванням, кіберхейтом, прокрастинацією та цифровою втомою.

Опитування підтвердило, що значна частина державних службовців регулярно перебуває в інтернет-просторі не лише з професійною, а й з особистою метою. Водночас понад 40% з них зізналися у щоденному відволіканні на неслужбові онлайн-активності, а майже 22% постійно відкладають виконання службових завдань на користь другорядного цифрового контенту. Це вказує на поширення діджитал-прокрастинації як

деструктивного чинника, що знижує продуктивність та ускладнює самоменеджмент державного службовця.

Однією з найгостріших проблем виявилося поширення кіберхейту – зневажливих висловлювань, принижень і ворожих дій у соціальних мережах, месенджерах, чатах і навіть у приватних повідомленнях. Кіберхейт часто стосується політичних тем, зовнішності, соціального статусу, гендеру і т. ін. Більшість респондентів визнають, що ці прояви викликають сильну емоційну реакцію: злість, засмучення, тривожність, що ускладнює збереження психологічної стійкості під час професійного функціонування.

Встановлено, що крему загрозу становить не лише переживання кібернасильства, а й участь самих державних службовців в агресивних діях у кіберпросторі. Значна частина респондентів зізналася у поширенні образливого контенту, що є показником цифрової незрілості, низької етичної стійкості та потреби в нормативній регуляції поведінки в мережі.

Виявлено також низький рівень інституційної довіри: респонденти не готові звертатися до керівництва, поліції чи психологічних служб у випадку кіберконфлікту, натомість переважно покладаються на неформальні джерела підтримки – друзів, родину або ні на кого. Це свідчить про потребу створення механізмів внутрішньої підтримки, підвищення довіри до служб безпеки та розвитку психологічної компетентності. Серед запитів на підтримку переважають освітні (тренінги, інформаційні ресурси), технічні (блокування, налаштування безпеки) та юридичні потреби. Це вказує на важливість формування інституційних програм цифрової обізнаності та професійної підготовки в контексті кібербезпеки.

4. Доведено, що професійна діяльність державних службовців у кіберпросторі детермінується сукупністю чинників: індивідуально-психологічних, соціально-комунікативних та організаційно-інституційних. Їх врахування є критично необхідним для формування цілісної системи цифрової адаптації та безпеки державної служби в умовах сучасних викликів.

5. В межах розроблених та обґрунтованих рекомендації щодо

підвищення ефективності управління персоналом на державній службі констатується ряд важливих положень.

Презентовано адаптовану модель імплементації кращих міжнародних практик щодо взаємодії державних службовців у кіберпросторі. Виокремлено успішні підходи Нідерландів, Великої Британії, Канади, Болгарії, Індії, Естонії, а також досвід Сінгапуру та Данії, де механізми «м'якого підштовхування» реалізуються через тонкі інтервенції у формі самопідказок у цифровому та організаційному просторах, використанні соціальних норм як підсилювачів відповідальності, а також застосуванні сенсорних сигналів (колір, структура документа), що підвищують ймовірність позитивної поведінкової реакції. Ефективність таких інтервенцій підтверджується результатами рандомізованих контрольованих експериментів (RCT), що дозволяють кількісно вимірювати поведінкові зміни, пов'язані із запровадженням конкретних інформаційних форматів або повідомлень.

Логічним продовженням імплементації міжнародного досвіду став розвиток кіберпсихологічної компетентності державних службовців як ключової умови підвищення їхньої цифрово-поведінкової зрілості. Визначено її структуру (когнітивний, емоційно-регулятивний, поведінковий, етичний компоненти), проаналізовано виявлені вразливості (низька стресостійкість, схильність до реактивної агресії, відсутність навичок протидії кібербулінгу). Запропоновано поетапну систему формування цієї компетентності через навчальні модулі, роботу HR-психологів, інтерактивні симуляції та моніторинг показників цифрової поведінки. Розроблено матрицю індикаторів для оцінювання рівня компетентності, що поєднує кількісні та якісні методи.

Вимірювання цифровоповедінкової зрілості інтегрується у кадрову політику як інструмент забезпечення безпечного, етичного та психологічно стійкого цифрового середовища.

Розкрито пропедевтику кібербулінгу та кіберхейту як складову цифрової безпеки кадрової політики. Визначено основні форми цифрової агресії, причини її поширення у держсекторі та проаналізовано ризики для

ефективності роботи колективу (зниження довіри, вигорання, деструкція комунікаційних зв’язків). Запропоновано науково обґрунтовані моделі інституційних механізмів реагування, що передбачають створення протоколів дій, відповідальних HR-підрозділів, цифрових омбудсменів, а також реалізацію комунікаційних кампаній нульової толерантності до цифрової агресії з використанням освітніх платформ, чат-ботів та анонімних форм повідомлення.

Перспективу подальших досліджень вбачаємо у напрямках вирішення проблем забезпечення інтеграції цифрової етики та кіберпсихологічної грамотності у систему управління персоналом, що сприятиме підвищенню стійкості державної служби до кіберзагроз, зміцнить довіру суспільства до публічної адміністрації та підвищить ефективність міжособистісної взаємодії у кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративне право України: підручник / Ю. П. Битяк (кер. авт. кол), І. М. Балакарева, І. В. Бойко та ін.; за заг. ред. Ю. П. Битяка. Харків: Право, 2020. 392 с.

2. Андрєєв А. В. Проблеми правового регулювання кадрового забезпечення державної служби України. дис. … докт. юрид. наук: 12.00.05. Київ, 2019. 417 с.

3. Андрєєва О. М. Електронне урядування: теорія та практика. навч. пос. К.: Авега. 2015. 228с.

4. Баранов О. А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання. *ІТ-право: проблеми та перспективи розвитку в Україні*. 2017. С. 18-42.

5. Барікова А. А. Електронна держава: нова ефективність урядування : монографія. Київ: Юрінком Інтер, 2016. 224 с.

6. Батир Ю., Помаза-Пономаренко А., Лопатченко І. Електронне урядування розвитком сучасних міст. *Вісник національного університету цивільного захисту України. Серія «Державне управління»*. 2021. № 2(15). С. 278–279.

7. Бєликов К. Організаційно-правові проблеми формування державної інформаційної політики України. *Право України*. 2004. № 10. С. 125-129.

8. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47 59.

9. Боссарт Д., Демке К. Державна служба у країнах-кандидатах до вступу до ЄС: нові тенденції та вплив інтеграційного процесу (пер. з англ. О. М. Шаленко). Київ: Міленіум, 2004. 128 с.

10. Буртник Х. Правові позиції Європейського Суду з прав людини щодо доступу до публічної інформації: аналітичний огляд. Рада Європи, 2020. 138 с.

11. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. Львів : Вид. Магнолія-2006, 2013. 432 с.

12. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

13. Варіативність соціалізації особистості в умовах сучасного інформаційного суспільства: монографія / авт. колектив : Н. М. Токарева, А. В. Шамне, О. О. Халік та ін.; ред. Н. М. Токаревої. Київ : ТОВ НВП «Інтерсервіс», 2017. 220 с.

14. Васьківська С. Психологічний імунітет як показник адаптаційних ресурсів особистості. *Гуманітарний вісник Державного вищого навчального закладу «Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди». Педагогіка. Психологія. Філософія : зб. наукових праць. М-во освіти і науки, молоді та спорту України, Переяслав-Хмельн. держ. пед. унт ім. Г. Сковороди. Переяслав-Хмельницький*, 2012. Вип. 25. С. 241–246.

15. Вербицький П. Взаємодія органів державної влади і мас-медіа як категорія науки про соціальні комунікації. *Діалог: медіа студії*. 2016. № 22. С. 17–28.

16. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. *Цифрова трансформація кібербезпеки: науково-практична інтернет-конференція, 20 квітня 2022, Державний університет телекомунікацій; Навчально-наукового інститут захисту інформації*. Київ, 2022. С. 31–33.

17. Вітлінський В. В. Штучний інтелект у системі прийняття управлінських рішень. *Нейронечіткі технології моделювання в економіці*. 2012. № 1. С. 97–118.

18. Войскунский А. Е. Киберпсихология в прошлом, настоящем и будущем. *Журнал практического психолога*. 2010. № 4. С. 7–16.

19. Гаврада І. О. Політика органів державної влади щодо ЗМІ в Україні: проблеми взаємодії: дис. канд. політ. наук: 23.00.02 / Чернівецький національний ун-т ім. Юрія Федьковича. Чернівці, 2007. 224 с.

20. Гайдученко С. О. Формування інноваційної технології оцінювання в управлінні персоналом. державної служби. : автореф. дис. … канд. наук з держ. упр. : 25.00.03. Дніпропетровськ, 2010. 20 с.

21. Галаджун З. В. Правові норми журналістики України : навч. посібник. Львів: СПОЛОМ, 2016. 190 с.

22. Галлін Д., Манчіні П. Сучасні медіасистеми: три моделі відносин ЗМІ та політики / Переклад з англ. О. Насика. К. : Наука, 2008. 320 с.

23. Гаркуша А.Т. Адміністративно-правовий статус Національного агентства України з питань державної служби: дис.. … канд.. юрид наук: 12.00.07. Одеса, 2017. 248 с.

24. Гетьман А. П., Атаманова Ю. Є., Мілаш В. С. Правове регулювання відносин у мережі інтернет: монографія. Харків, 2016. 360 с.

25. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118–129.

26. Головій В. М. Механізми взаємодії влади та ЗМІ в контексті становлення громаданського суспільства в Україні: автореф. дис... канд. наук з держ. управління: 25.00.02 / Класичний приватний ун-т. Запоріжжя, 2009. 20 с.

27. Голубь В. В. Ефективна держава у контексті суспільних трансформацій. *Грані.* 2013. № 12. С. 154-159.

28. Гончарук О. Б., Савичук Н. О. Поняття механізмів державного управління та їх практичне значення. *Інвестиції: практика та досвід*. 2021. № 7. С. 77–83.

29. Гриценко А. А. Цифровізація як сучасний тренд економічного та суспільного розвитку. *Цифрова економіка: зб. матеріалів II Нац. наук.-метод. конф*. Київ: КНЕУ, 2019. С. 685–690.

30. Грицишен Д. О., Євдокимов В. В., Савчук С. О., Корзун С. В. Стратегія інтеграції державної політики протидії кіберзлочинності в європейську систему кібербезпеки: монографія. Житомир: ТОВ «Видавничий дім “Бук-Друк”». 2024. 312 с.

31. Грищук Р. В. Основи кібернетичної безпеки : монографія / За заг. ред. проф. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.

32. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 (ISO/IEC 27001:2005, MOD). Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги [Галузевий стандарт України]. К.: Національний банк України. 2010. 49 с.

33. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 (ISO/IEC 27002:2005, MOD). Інформаційні технології. Методи захисту. Звід правил управління інформаційною безпекою [Галузевий стандарт України]. К.: Національний банк України. 2010. 163 с.

34. Гудімова А. Х. Поведінкові патерни користувачів соціальних мереж як умова їх психологічного благополуччя. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 053 Психологія. Одеський національний університет імені І. І. Мечникова. (м. Одеса), 2021. 243 с.

35. Данильян О. Г., Дзьобань О. П. Віртуальна реальність і кіберпростір як атрибути сучасного суспільства. *Інформація і право*. 2020. № 4(35). С. 9-21.

36. Данильян, О. Г., Дзьобань, О. П. Методологія наукових досліджень : підручник. Харків : Право, 2019. 368 с.

37. Демкова М. С., Коліушко І. Б. Електронне урядування – шлях до ефективності та прозорості державного управління. *Інформаційне суспільство. Шлях України*. К.: Бібліотека інформаційного суспільства. 2004. С. 138-143.

38. Державне управління: проблеми адміністративно-правової теорії та практики / За заг. ред. В. Б. Авер'янова. Київ: Факт, 2003. 384 с.

39. Дженюк Н., Євсеєв С., Лазуренко Б., Сєрков О., Касілов О. Спосіб захисту інформації в кіберфізичному просторі. *Сучасні інформаційні системи*. 2023. Т. 7. № 4. С. 80–86.

40. Дзьобань О. П. Методологія, організація та технологія наукових досліджень : навч. посіб. для аспірантів. ДНУ «Ін-т інформації, безпеки і права Нац. академії прав. наук України». Київ; Одеса : Фенікс, 2025. 284 с.

41. Дрешпак В. М. Комунікації в публічному управлінні : навч. посіб. Д. : ДРІДУ НАДУ, 2015. 168 с.

42. Дубов Д. В. Підходи до формування тезауруса в галузі кібербезпеки. *Політичний менеджмент*. 2010. № 5. С. 19–30.

43. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. К. : НІСД, 2014. 328 с.

44. Дульська І. В. Цифрові технології як каталізатор економічного зростання. *Економіка і прогнозування*. 2015. № 2. С. 119-133.

45. Електронне урядування в Україні: аналіз та рекомендації. Результати дослідження / О. А. Баранов, І. Б. Жиляєв, М. С. Демкова та ін.; за ред. І. Г. Малюкової. К.: ООО «Поліграф-Плюс», 2007. 254 с.

46. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А. І. Семенченка, В. М. Дрешпака. Частина 2. К. : ФОП Москаленко О. М., 2017. 72 с.

47. Електронне урядування: конституційно-правове дослідження / Авт. кол.: Романчук О. З., Бисага Ю. М., Берч В. В., Нечипорук Г. Ю., Чечерський В. І. К., 2016. 172 с.

48. Електронний уряд. Науково-практичний довідник / Уклад.: Чукут С. А., Клименко І. В., Линьов К. О. [Електронний ресурс]. Режим доступу: URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/Elektronnij-dovidnik.pdf

49. Емран Р. Держава у смартфоні. *Харківський національний економічний університет ім. С. Кузнеця*. Харків. 2021. С. 21-22.

50. Енциклопедичний словник з державного управління / за ред. Ю. В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна; уклад. В. Д. Бакуменко, А. М. Михненко та ін. Київ : НАДУ, 2010. 820 с.

51. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія / О. Д. Довгань, І. М. Доронін; НАПрН України, НДІІП. Київ : Видавничий дім «АртЕк», 2017. 107 с.

52. Ефективність державного управління / Авт. кол.: Ю. Бажал, О. Кілієвич, О. Мертенс та ін.; за заг. ред. І. Розпутенка. К.: Вид-во «К. І. С», 2002. 420 с.

53. Ємельяненко О. М. Електронний уряд: інноваційні підходи до політики і управління в інформаційному суспільстві: автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.02 «Політичні інститути та процеси». Одеса, 2008. 20 с.

54. Ємельянов В. М. Проблеми та перспективи розвитку електронного урядування в Україні. *Наукові праці Чорноморського державного університету ім. Петра Могили комплексу «Києво-Могилянська академія»*. 2016. № 269. С. 11–17.

55. Єфремов М. Ф., Єфремов Ю. М. Штучний інтелект, історія та перспективи розвитку. *Вісник ЖДТУ. Серія «Технічні науки».* 2008. № 2(45). С. 123-126.

56. Жовнірчик Я. Ф., Квасюк В. В. Електронне врядування та електронна демократія стосовно децентралізації в Україні: стратегії реалізації та розвитку. *Інвестиції: практика та досвід*. 2020. № 1. С. 106–115.

57. Забейворота Т. Сучасна концепція е-врядування як основа модернізації системи державного управління. *Актуальні проблеми державного управління*. 2017. №. 1(51). С. 35–42.

58. Іванків І. І. Соціально-психологічні особливості кіберпростору. *Молодий вчений*. 2015. № 6(3). С. 96–100.

59. Інституціоналізація публічної служби в Україні: теорія і практика : [*монографія*] / Авт. кол.: Н. О. Алюшина, Н. С. Наулік, С. А. Романюк та ін.; за заг. ред. проф. С. К. Хаджирадєвої. К.: Видавничий дім «АртЕк», 2022. 342 с.

60. Інформаційна безпека держави: підручник [В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник та ін.] ; в 2 т. Т. 2. К., 2016. 328 с.

61. Іртищева І. О., Крамаренко І. С., Богатирьов К. О., Гришина Н. В., Купчишина О. А., Ракіпов В. Р. Форсайт цифрової трансформації національної

економіки та її вплив на забезпечення інноваційного розвитку. *Актуальні проблеми інноваційної економіки та права*. 2023. № 5. С. 96–101.

62. Кагановська Т. Є. Кадрове забезпечення державного управління в Україні: монографія. Харків: ХНУ імені В.Н. Каразіна, 2010. 330 с.

63. Каплій О. В. Правовий вплив недержавних засобів масової інформації на формування правової культури та правомірної поведінки громадян. Правовий вплив на неправомірну поведінку: актуальні грані: монографія / за ред. проф. О. В. Козаченка, проф. Є. Л. Стрельцова. Миколаїв: Іліон, 2016. 768 с.

64. Кармінська-Бєлоброва М. В. Особливості сучасних концепцій управління персоналом. *Вісник Національного технічного університету «ХПІ»: зб. наук. пр*. Харків : НТУ «ХПІ». 2018. № 37 (1313). С. 36–40.

65. Карпа М. І. Методи управління кадровими процесами у контексті становлення публічної служби в Україні. *Ефективність державного управління*. 2013. Вип. 37. С. 354–362.

66. Квітка С. А. Електронне врядування як інноваційний механізм взаємодії влади, бізнесу та громадянського суспільства: зарубіжний досвід та передумови розвитку в Україні. *Аспекти публічного управління*. 2015. № 9. С. 26–34.

67. Кирилюк А. В. Юридична природа мережі Інтернет: історія створення, будова та можливості. *Часопис цивілістики*, 2014. № 17. С. 204–208.

68. Кияниця Є. О. Структурний підхід до формування медіалогії як науково-практичного напряму. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Соціальні комунікації*. Том 30(69). № 2 Ч. 2. 2019. С. 146-150.

69. Кіберпсихологія у вимірах сучасного дискурсу : монографія / автор. кол.: С. Хаджирадєва, Ю. Левін, М. Тодорова; за заг. ред. С. Хаджирадєвої. Одеса : Астропринт, 2024. 240 с.

70. Коброслі А. Х. Соціальні мережі та психологічне благополуччя підлітків: переваги та ризики. *Теоретичні і прикладні проблеми психології*. 2019. № 2. С. 194–203.

71. Кондрашова Л. В., Друзь З. В., Білоконна Н. І., Мірошник З. М. Формування творчої особистості в процесі навчання: теорія, практика, досвід : монографічний посібник. Кривий Ріг – Київ, 2009. 559 с.

72. Конституційне право України : навч. посіб. / автор. кол.: О. Г. Остапенко, В. В. Сергієнко. Харків : ХНЕУ ім. С. Кузнеця, 2020. 260 с.

73. Конституція України. Прийнята Верховною Радою 28 червня 1996 р. Відомості Верховної Ради України (ВВР). 1996. № 30. ст. 141.

74. Концепція розвитку електронного урядування в Україні / О. А. Баранов, М. С. Демкова, С. В. Дзюба та ін.; за ред. А. І. Семенченко. К., 2009. 398 с.

75. Копан О. В. Словник термінів з кібербезпеки. К. : «Аванпост-Прим», 2012. 214 с.

76. Костенко І. Основні принципи електронного урядування. *Часопис Київського університету права*. 2019. № 2019/4. С. 118–119.

77. Костирєв А. Г. Роль засобів масової інформації в процесі демократичного розвитку суспільства : автореф. дис ... канд. політ. наук: 23.00.02. Київ : Б.в., 2003. 17 с.

78. Кохан В. П. Цифрова компетентність громадян Європейського Союзу [Електронний ресурс]. Режим доступу: https://ndipzir.org.ua/wp-content/uploads/2020/06/Tezy_05.06.20/ _13.pdf

79. Кравченко О. О. Управління державною службою в Україні: організаційно-правові засади: дис. … канд. юрид. наук: 12.00.07. Харків, 2010. 213 с.

80. Крушельницька О. В. Мельничук Д. П. Управління персоналом: навч. посіб. Київ: Кондор, 2005. 308 с.

81. Кубко А. Є. Державні інтереси і відповідальність держави: деякі питання співвідношення. *Часопис Київського університету права*. 2019/4. [Електронний ресурс]. Режим доступу: https://chasprava.com.ua/index.php/journal/article/download/ 107/95/

82. Ларина Е. С. Социальная физика Девида Пентланда и поведенческие войны [Електронний ресурс]. 2016. Режим доступу: http://spkurdyumov.ru/biology/socialnaya-fizika-devida-pentlandaipovedenches

83. Лашкіна М. Г. Взаємовідносини влади і ЗМІ: нові виклики часу. *Актуальні проблеми державного управління на новому етапі державотворення: матеріали наук.-практ. конф. за міжнар. участю. Київ, 31 трав. 2005 р. : у 2 т. / за заг. ред. В. І. Лугового, В. М. Князєва*. К. : Вид-во НАДУ, 2005. Т. 1. С. 237–238.

84. Лесечко М. Д. Основи системного підходу: теорія, методологія, практика: Навч. посіб. Львів: ЛРІДУ НАДУ, 2002. 300 с.

85. Ліпкан В. А., Харченко Л. С., Логінов О. В. Інформаційна безпека України: глосарій. Київ : Вид. Кондор, 2004. 382 с.

86. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. № 5. С. 174–180.

87. Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с.

88. Лопушняк Г. С., Миляник Р. В. Вплив цифрових технологій на формування компетенцій управлінського персоналу. *Інвестиції: практика та досвід*. 2019. № 24. С. 10-16.

89. Лук'янова Г. Ю., Венглінська А. С. Особливості впровадження електронного урядування в органах виконавчої влади України. Електронне наукове видання «Аналітично-порівняльне правознавство». [Електронний ресурс]. Режим доступу: http://journal-app.uzhnu.edu.ua/article/view/255113/252218

90. Лучинкина А. И. Психология человека в Интернете. К. : ТОВ «Інформаційні системи», 2012. 200 с.

91. Майданник О. О. Конституційне право України: навч. посіб. К. : Алерта, 2011. 380 с.

92. Максименко С. Д. Актуальні проблеми генетичної психології. *Актуальні проблеми психології: зб. наук. пр. Ін-ту психології імені Г. С. Костюка НАПН України*. К., 2019. Т. VIII: Психологічна теорія і технологія навчання. Вип. 10. С. 8–20.

93. Максимова Н. Ю. Психологія адиктивної поведінки: навчальний посібник. К. : Київський університет, 2002. 308 с.

94. Мальцева О. І. Кіберсоціалізація як особливий вид соціалізації особистості. *Вісник Луганського національного університету імені Тараса Шевченка. Педагогічні науки*. 2020. № 2(333), Ч. 2. С. 190–199.

95. Манжай О. В Правові заходи захисту інформації. Харків : Панов, 2020. 162 с.

96. Матвейчук Л. О., Польовий П. В. Цифрова компетентність публічних службовців. [Електронний ресурс]. Режим доступу: https://pubadm.vernads kyjournals.in.ua/journals/2022/2.pdf

97. Матюхіна Н. П. Управління персоналом органів внутрішніх справ України (Теоретичні та прикладні аспекти): монографія / за заг. ред. Бандурки О. М. Харків: Вид-во Ун-ту внутр. справ, 1999. 287 с.

98. Махній М. М. Мережеве суспільство : кіберпсихологічний путівник. Київ: Academia.edu, 2018. 176 с.

99. Машбиць Ю. І. Психологічні механізми і технологія навчання. К.: Інтерсервіс, 2019. 208 с.

100. Мельник А. Ф., Оболенський О. Ю., Васіна А. Ю., Гордієнко Л. Ю. Державне управління: навч. посіб. Київ: Знання-Прес, 2003. 343 с.

101. Методологія наукових досліджень : підручник / Авт. кол.: О. Г. Данильян,. О. П. Дзьобань. Харків : Право, 2019. 368 с.

102. Методологія наукових досліджень та приклади її використання: навч. посіб. К.: НУХТ, 2022. 385 с.

103. Министерството на вътрешните работи. Етичен кодекс за поведение на държавните служители в Министерството на вътрешните работи. Режим

доступу: https://legal-tech.bg/featured_item/kodeks-za-povedenie-na-sluzhitelite-v-drzhavnata-administratsiya/

104. Министерството на вътрешните работи. Заповед № 8121з-1169 от 23 август 2024 г. Относно изменение и допълнение на етичния кодекс за поведение на държавните служители в Министерството на вътрешните работи. Режим доступу: https://lex.bg/bg/laws_stoyan/ldoc/2137245285

105. Михайловська О. В. Наукові підходи до розуміння сутності поняття «взаємодія» в системі «влада-громадськість». *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2021. № 2. С. 71–75.

106. Мільо В. Ю. Проблеми правового регулювання діяльності «нових медіа». *Інформаційна безпека людини, суспільства, держави*. 2017. № 1(21). С. 114–123.

107. Міхровська М. С. Цифрове врядування як новий рівень взаємодії держави та суспільства. *Юридичний науковий електронний журнал*. № 7. 2020. С. 272–275.

108. Моляко В. О. Психологічна готовність до творчої праці. Київ : Знання, 1989. 48 с.

109. Мохор В., Гончар С., Дибах О. Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури. *Ядерна та радіаційна безпека*. 2019. № 2(82). С. 64–79.

110. Мурасов Р., Мельник Я. Оцінювання захищеності кіберпростору об’єктів критичної інфраструктури України. *Сучасні інформаційні технології у сфері безпеки та оборони*. Київ, Україна, 2024. № 46(1). С. 41–44.

111. Наумкина С., Пилипенко В., Привалов Ю. Социально-политическая эффективность управленческой деятельности. К.: Стилос, 1999. 141 с.

112. Національна безпека в контексті європейської інтеграції України: підручник / Г. П. Ситник, М. Г. Орел; за ред. Г. П. Ситника. Київ: Міжрегіональна Академія управління персоналом, 2021. 372 с.

113. Немеш О. М. Віртуальна діяльність особистості: структура та динаміка психологічного аналізу: монографія. К. : Слово, 2017. 391 с.

114. Нерсесян Л. С., Хавин А. Б. Прогнозирование готовности к экстренному действию в состоянии стресса. *Вопросы психологии*. 1980. № 5. С. 135–138.

115. Оксентюк С. Електронний уряд як головна складова електронного урядування. *Проблеми публічного управління та адміністрування на регіональному рівні*. 2019. № 5. С. 62-63.

116. Основи кіберпростору, кібербезпеки та кіберзахисту. / Авт. кол.: В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. К. : Видавництво Ліра-К, 2020. 554 с.

117. Піддубна Л. В. Кіберпростір як відображення трансформацій інформаційної економіки. *Вісник Житомирського державного університету імені Івана Франка. Філософські науки*, 2016. № 1. С. 107-112.

118. Плешаков В. А., Маркова В. К., Воинова О. И. Киберпедагогика : методология, теория и практика. Педагогика. 2021. № 4. С. 6–21.

119. Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави*. 2009. № 2(2). С. 80–85.

120. Послуги/Дія. Каталог послуг. [Електронний ресурс]. Режим доступу: URL:https://diia.gov.ua/services.

121. Почепцов Г. Г. Теория коммуникации. К. : Ваклер. 2003. 656 с.

122. Правові засади кібергігієни [Електронний ресурс]. Режим доступу: https://https://drive.google.com/file/d/1EPd677wdTA32Fbi5RzoobUk2CvcolQAW/view.

123. Про адміністративні послуги: Закон України від 06.09.2012 № 5203-VI // Офіційний вісник України. 2012. № 76. 44 с.

124. Про внесення змін до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство

України, посвідчують особу чи її спеціальний статус»: Закон України від 30.03.2021 № 1368-IX. *Офіційний вісник України*. 2021. № 33. С. 18.

125. Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста : Закон України від 23 вересня 1997 р. № 540/97-ВР [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/540/97-%D0%B2%D1%80#Text

126. Про державну службу: Закон України від 10.12.2015 р. № 889-VIII. [Електронний ресурс]. Режим доступу: URL: https://zakon.rada.gov.ua/laws/card/889-19.

127. Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-XII [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text

128. Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади : Указ Президента України від 1 серпня 2002 р. № 683/2002 [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/683/2002#Text

129. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. *Офіційний вісник України*. 2011. № 10. С. 29.

130. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. *Офіційний вісник України*. 2017. № 91. С. 5.

131. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. *Офіційний вісник України*. 2003. № 25. 106 с.

132. Про електронні комунікації : Закон України від 16 грудня 2020 р. № 1089-IX [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20#Text

133. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовтня 2017 р. № 2155-VIII [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text

134. Про затвердження Порядку сприяння проведенню громадської експертизи діяльності органів виконавчої влади : Постанова КМУ від 5

листопада 2008 р. № 976 [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/976-2008-%D0%BF#Text

135. Про затвердження Регламенту Кабінету Міністрів України : Постанова КМУ від 18 липня 2007 р. № 950 [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/950-2007-%D0%BF#Text

136. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 липня 1994 р. № 80/94-ВР [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%8#Text

137. Про заходи щодо подальшого забезпечення відкритості у діяльності органів виконавчої влади : Постанова КМУ від 29 серпня 2002 р. № 1302 [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1302-2002-%D0%BF#Text

138. Про Заяву Верховної Ради України про цінність свободи слова, гарантії діяльності журналістів і засобів масової інформації під час дії воєнного стану : Постанова Верховної Ради України від 14 квітня 2022 р. № 2190-IX [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2190-IX#Text

139. Про звернення громадян : Закон України від 2 жовтня 1996 р. № 393/96-ВР [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text

140. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

141. Про Концепцію Національної програми інформатизації: Схвалено Законом України від 4 лютого 1998 р. № 75/98-ВР [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/75/98%D0%B2%D1%#Text

142. Про критичну інфраструктуру : Закон України від 16 листопада 2021 р. № 1882-IX [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text

143. Про медіа : Закон України від 13 грудня 2022 р. № 2849-IX [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2849-20#Text

144. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text

145. Про національну систему конфіденційного зв'язку : Закон України від 10 січня 2002 р. № 2919-III [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2919-14#Text

146. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

147. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади : Постанова КМУ від 4 січня 2002 р. № 3 [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF#Text

148. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Введено в дію Указом Президента України від 28 грудня 2021 р. № 685/2021 [Електронний документ]. Режим доступу: https://www.president.gov.ua /documents/6852021-41069.

149. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України 25 лютого 2017 р. № 47/2017 [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/47/#Text

150. Про роботу центральних і місцевих органів виконавчої влади щодо забезпечення відкритості у своїй діяльності, зв'язків з громадськістю та взаємодії з засобами масової інформації : Розпорядження КМУ від 18 жовтня 2004 р. № 759-р [Електронний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/759-2004-%D1%80#Text

151. Про схвалення Концепції розвитку електронного урядування в Україні : Схвалено розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р [Електронний документ]. Режим доступу: https://zakon. rada.gov.ua/laws/show/649-2017-%D1%80#Text

152. Про схвалення Концепції розвитку цифрової економіки та суспільства україни на 2018-2020 роки та затвердження плану заходів щодо її реалізації: розпорядження кабінету міністрів України від 17.01.2018р. № 67-р. URL: http://zakon.rada.gov.ua/laws/show/67-2018%D1%80.

153. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Схвалено розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р [Електронний документ]. Режим доступу: https://www.kmu. gov.ua/npas/246420577

154. Прокопенко С. Л. Проблеми та перспективи цифровізації адміністративних послуг в Україні. *Інвестиції: практика та досвід.* 2024. № 12. С. 235–240.

155. Проценко Д. В. Розвиток законодавства України у сфері регулювання діяльності ЗМІ. *Наукові записки НаУКМА. Юридичні науки*. 2012. Т. 129. С. 88–92.

156. Психологія адиктивної поведінки: методичні рекомендації. Чернігів: ЧНПУ імені Т. Г. Шевченка, 2010. 84 с.

157. Публічна політика в процесах реформування системи державного управління України / С. О. Телешун, С. В. Ситник, І.В. Рейтерович, О. Г. Пухкал. НАДУ, 2016. 192 с.

158. Публічна політика та суспільні зміни в Україні в контексті євроінтеграції : монографія / авт. кол. : С. О. Телешун, С. В. Ситник, І. В. Рейтерович, О. Г. Пухкал та ін. ; за заг. ред. С. О. Телешуна, д-ра політ. наук, проф. Київ : НАДУ, 2017. 248 с.

159. Публічне управління в забезпеченні сталого (збалансованого) розвитку: навч. посіб / авт. кол. : Т. К. Гречко, С. А. Лісовський, С. А. Романюк, Л. Г. Руденко. Херсон: Грінь ДС, 2015. 264 с.

160. Пчелянський Д. П., Воінова С. А. Штучний інтелект: перспективи та тенденції розвитку. *Automation of technological and business processes*, 2019. № 11(3). С. 59–64.

161. Размєтаєва Ю. С. Електронне урядування як складник демократії в інформаційному суспільстві. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. Том 31 (70). № 1. 2020. С. 37–41.

162. Рибка С. В., Кільчицький Є. В., Післегін О. М. Кіберпростір, управління інфраструктурою, кібербезпека. *Стратегічна панорама*. 2015. № 1. С. 126–134.

163. Роєнко В. О. Форми і сфери прояву соціальних стереотипів в умовах кіберпростору та поза його межами. *Філософія і політологія в контексті сучасної культури*, 2014. № 8. С. 103–107.

164. Рожило М. А. Теребус О. Л. Проблема саморегуляції українських медіа. *Вчені записки ТНУ імені В.І. Вернадського. Серія: "Філологія. Журналістика"*. 2021. № 3/41. С. 239–244

165. Романчук О. З., Бисага Ю. М., Берч В. В., Нечипорук Г. Ю., Чечерський В. І. Електронне урядування: конституційно-правове досліджння : Монографія. Ужгород. РІК-У. 2021. 196 с.

166. Савчук С. О. Виклики та можливості інтеграції України в систему кібербезпеки ЄС. *Економіка, управління та адміністрування*. 2024. № 2. С. 198-203.

167. Самойленко О., Лисак П. Психологічна готовність особистості як предмет наукового дослідження. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія : Психологічні науки*. 2019. № 2(13). С. 232–241.

168. Саннікова О. П. Толерантність до невизначеності як предиктор прийняття рішень особистістю. *Вісник післядипломної освіти: збірник наукових праць*. К. : НАПНУ, 2020. С. 98–123.

169. Семенченко А. І. Електронне урядування в Україні: проблеми та шляхи вирішення. *Міжнародний фаховий журнал «Електронне урядування»*. 2010. № 1. С. 8–14.

170. Семенченко А. І. Електронне урядування та електронна демократія : навчальний посібник. Київ: ФОП Москаленко О. М., 2017. 72 с.

171. Семенченко А. І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України. Київ : НАДУ, 2008. 429 с.

172. Сенченко Н. А. Інтернет як соціокультурний феномен. *Культура народов Причерноморья*. 2014. № 267. С. 156–159.

173. Ситник Г. П. Національна безпека України: теорія і практика : навч. посібник. К. : «Кондор», 2007. 616 с.

174. Скакун О. Ф. Теорія права і держави. Київ, 2016. 520 с.

175. Смульсон М. Л. Психологічні механізми становлення суб'єктності дорослих у віртуальному просторі: монографія. Київ-Львів : Видавець Вікторія Кундельська, 2021. 180 с.

176. Сніцаренко П. М., Саричев Ю. О., Рогов П. Д. Методика оцінки рівня деструктивного інформаційного впливу на об'єкти інформаційної інфраструктури держави. *Збірник наукових праць ВІТІ ДУТ*. № 1. 2014. С. 88–96.

177. Сніцаренко П., Саричев Ю., Гордійчук В. Сутність кіберпростору та його взаємозв'язок із кібернетичним простором. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 50(2), С. 5–10.

178. Соловйова О. М., Ковальчук Д. Р., Кундій А. Ю. Перспективи та проблеми впровадження електронного урядування в Україні. *Юридичний науковий електронний журнал*. 2021. № 11. С. 109–112.

179. Соціальна інженерія в контексті кібернетичної безпеки України (сучасні технології та шляхи захисту): навч. посіб. / [Ю. Г. Куцан, О. М. Богданов, В. М. Петрик, Д. В. Пахольченко, А. В. Давидюк] / за заг. ред. В. М. Петрика. К., 2017. 80 с.

180. Спасібов Д. Електронне урядування в системі сучасних концепцій публічного управління. *Теорія та практика державного управління*. 2018. №2(61). URL: http://www.kbuapa.kharkov.ua/e-book/tpdu/20182/index.html

181. Сталий розвиток і цифрові інновації: монографія / за заг. ред. Буркінського Б. В., Назаренко О. А., Лайко О. І., Хаджирадєвої С. К. та ін.; НАН України, МОН України, ДУ «Ін-т ринку та економ.-екол. дослідж.», Державний університет інтелектуальних технологій і зв'язку. Одеса, ДУ ІРЕЕД НАНУ», 2024. 543 с.

182. Стратегія інтеграції державної політики протидії кіберзлочинності в європейську систему кібербезпеки: монографія / За заг. ред. В. В. Євдокимова, Д. О. Грицишена. Житомир: «Видавничий дім "Бук-друк"». 2024. 420 с.

183. Стратегія реформування державного управління України на 2022-2025 роки : Розпорядження Кабінету Міністрів України від 21.07.2021 р. № 831-р. URL: https://zakon.rada.gov. ua/laws/show/831-2021-%D1%80#n9

184. Сундук, А. М. Управління розвитком національної економіки в умовах глобальних викликів і загроз. Київ : Логос, 2012. 302 с.

185. Сучасна культурологія: актуалізація теоретико-практичних вимірів: колективна монографія. / За загал. ред. проф. Ю. С. Сабадаш; редактори укладачі: проф. Ю. С. Сабадаш, проф. І. В. Петрова. Київ : Вид-во Ліра-К, 2019. 308 с.

186. Съвет на министрите на Република България. Кодекс за поведение на служителите в държавната администрация: Приет с ПМС № 57 от 02.04.2020 г. Режим доступу: https://legal-tech.bg/featured_item/kodeks-za-povedenie-na-sluzhitelite-v-drzhavnata-administratsiya.

187. Телешун Я. С. Функціонування фінансово-політичних груп в нестабільному середовищі: реалії України. *Гілея: науковий вісник. Збірник наукових праць / Гол. Рел. В. М. Вашкевич*. К. : «Видавництво «Гілея», 2016. Вип.113(10). С. 401–406.

188. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. № 1. С. 75–86.

189. Україна: інформація і свобода слова: збірник законодавчих актів, нормативних документів та статей фахівців / упоряд. А. М. Задворний. К. : Молодь, 1997. 832 с.

190. Управління змінами в публічній сфері: *навч.-метод. посіб.* / Авт. кол.: С. К. Хаджирадєва, С. А. Романюк, В. А. Грабовський, І. М. Фищук, Д. М. Букатова. Київ : НАДУ, 2018. 192 с.

191. Управління персоналом в органах публічної влади : навч. посіб. / С. М. Серьогін та ін. Дніпро. : ДРІДУ НАДУ, 2019. 200 с.

192. Управління персоналом у публічній службі : навч. посіб. для здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 281 «Публічне управління та адміністрування» / Авт. кол. Хаджирадєва С. К., Рачинський А. П., Васильєва О. І., Ларіна Н. Б.; за заг. ред. С. К. Хаджирадєвої. Миколаїв : Ємельянова Т. В., 2020. 212 с.

193. Федоренко В. Л. Конституційне право України : підруч. / До 20-ої річниці Конституції України та 25-ої річниці незалежності України. К. : Видавництво Ліра-К, 2016. 616 с.

194. Федорова І. І. Інформаційна ера: глобальні трансформації культурного простору. *Вісник Національного технічного університету України «КПІ». Філософія. Психологія. Педагогіка*, 2015. № 2(44). С. 98–104.

195. Форос Г. В., Жогов В. С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. № 33. С. 128–134.

196. Фрейд З. Вступ до психоаналізу. Нові висновки. Навчальна книга. К. : Богдан. 2021. 552 с.

197. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2(5). С. 162–169.

198. Фурашев В. Питання законодавчого визначення понятійнокатегоріального апарату у сфері інформаційної безпеки. *Інформація і право*. 2012. № 1(4). С. 46–55.

199. Хміль Ф. І. Управління персоналом: підручник. К. : Академвидав, 2006. 488 с.

200. Хорватова О. О., Пухір Ю. І. Деякі аспекти правового регулювання законної діяльності журналіста в сучасних умовах. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. Вип. 81. Ч. 2. 2024. С. 366–371.

201. Цимбалюк В. С. Мас-медіа-право в інформаційному суспільстві. *Інформація і право*. 2011. № 1(1). С. 30–33.

202. Цимбалюк В. С. Основи інформаційного права України. К. : Знання, 2004. 274 с.

203. Чебикін О. Я., Павлова І. Г. Становлення емоційної зрілості особистості : монографія. Одеса: ПНЦ АПН України, 2009. 238 с.

204. Чечель О. Ю. Розвиток інформаційного простору та Е-уряду в Україні. *Теорія та практика державного управління*. 2016. № 3. С. 74–81.

205. Чукут С. А. Роль сучасних засобів масової інформації в процесах державотворення (окремі аспекти). *Вісник УАДУ*. 1999. № 3. С. 158-167.

206. Чукут С. Сутність електронного уряду та принципи його організації. *Вісник УАДУ*. 2003. № 2. С. 429-433.

207. Энциклопедия кибернетики. Т.1: А – Л. (Под ред. Глушкова В. М.). К. : Головна редакция УРЕ, 1973. 583 с.

208. Юр’єва Л. М., Шорніков А. В. Новий інструмент у діагностиці кібер-залежності. *Український Вісник Психоневрології*. 2021. Т. 29. № 3(108). С. 57–62.

209. Юровська, В. В. Людиноцентристська концепція адміністративно-правової доктрини: філософський аспект нової ідеології адміністративного права. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2016. № 41. Т. 3. С. 96-102.

210. Яковенко Ю. Л. Модель відносин влади і масмедіа в Україні. *Регіональні студії: науковий збірник / редкол.: М. М. Палінчак (голов. ред.), І. М. Вегеш, Є. І. Гайданка та ін*. Ужгород : Видавничий дім «Гельветика», 2024. Вип. 37. С. 75–80.

211. Ajzen I. The Theory of Planned Behavior // Organizational Behavior and Human Decision Processes. 1991. T. 50, No 2. P. 179–211. Режим доступу: https://doi.org/10.1016/0749-5978(91)90020-T (дата звернення: 15.08.2025).

212. An Introduction to Cyberpsychology. Edited by Irene Connolly, Marion Palmer, Hannah Barton and Gráinne Kirwan. Routledge, 2016. 348 p.

213. Anderson C. L., Agarwal R. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*. 2010. T.34, No 3. P. 613–643.

214. Argaman O. Linguistic Markers and Emotional intensity. *Journal of Psycholinguistic Research*, 2010. No 39(2). P. 89–99.

215. Ashenden D., Sasse M. A. CISOs and organisational culture: Their own worst enemy? *Computers & Security*. 2013. T. 39. P. 396–405.

216. Attrill-Smith A., Fullwood C., Keep M., & Kuss D. J. (Eds.). The Oxford handbook of cyberpsychology. Oxford University Press, 2019. 720 p.

217. Baccarella C. V., Wagner T. F., Kietzmann J. H., McCarthy I. P. Social media? It's serious! Understanding the dark side of social media. *European Management Journal*. 2018. T.36. № 4. P. 431–438.

218. Bandura A. Social learning theory. Englewood Cliffsю NJ: Prentice Hall. 1977. 247 p.

219. Bard A., Soderqvist J. Netocracy: The New Power Elite and Life After Capitalism. Ft Pr; First Edition. 2002. 288 p.

220. Barsky A. J.; Klerman G. L. Overview: Hypochondriasis, bodily complaints, and somatic styles. *American Journal of Psychiatry*. 1983. No 140(3). P. 273–283.

221. Behavioural Insights Team. 2019. Режим доступу: https://www.bi.team/ (дата звернення 15.08.2025).

222. Behavioural Insights Team. Using Behavioural Science to Improve Digital Conduct in Government Services: Internal briefing report (unpublished). 2021. Режим доступу: https://www.bi.team/publications/behavioural-government/ (дата звернення 09.04.2025).

223. Behavioural Leeway. Soft Governance in Digital Communication. 2022. Режим доступу: https://behaviouralleeway.com/nudging-in-civil-service (дата звернення 23.07.2025).

224. Behavioural Leeway. Theory and Practice of Social Norm Nudging. 2023. Режим доступу: https://behaviouralleeway.com/theory-and-practice-of-social-norm-nudging/ (дата звернення 15.05.2025).

225. Bianchi F., Squazzoni F. Agent-Based Models in Sociology // Wiley Interdisciplinary Reviews: Computational Statistics. 2015. T. 7, № 4. Режим доступу: https://doi.org/10.1002/wics.1356 (дата звернення: 12.02.2025).

226. Bicchieri C. Norms in the Wild: How to Diagnose, Measure, and Change Social Norms. Oxford : Oxford University Press, 2016. Режим доступу: https://doi.org/10.1093/ACPROF:OSO/9780190622046.001.0001 (дата звернення 11.03.2025).

227. Bignel J. Media semiotics. An introduction. Manchester etc., 1997. 234 p.

228. Brooks S., Califf C. Social Media-Induced Technostress: Its Impact on the Job Performance of IT Professionals and the Moderating Role of Job Characteristics. *Computer Networks*. 2017. T. 114. P. 143–153.

229. Burger A., Schubert C., Bizer K. Nudging for Sustainability: The Use of Behavioural Economics in Environmental Policy. *Oxford Journal of Economic Policy*. 2015. T. 31. № 2. P. 231–252.

230. Canada School of Public Service. Digital Academy: Building digital skills in government. Ottawa : Government of Canada, 2022. Режим доступу: https://www.csps-efpc.gc.ca/digital (дата звернення: 15.01.2025).

231. Cattell R. B. The birth of the Society of Multivariate Experimental Psychology. *Journal of the History of the Behavioral Sciences,* 1990. No 26. P. 48–57.

232. Chio C., Freeman D. Machine Learning and Security: Protecting Systems with Data and Algorithms. Sebastopol, CA : O'Reilly Media, 2018. 397 p.

233. Cioffi-Revilla C. Introduction to Computational Social Science: Principles and Applications. London : Springer, 2014. Режим доступу: https://doi.org/10.1007/978-1-4471-5661-1 (дата звернення 08.02.2024).

234. Connor K. M., Davidson J. R. T. Development of a new resilience scale: The Connor-Davidson Resilience Scale (CD-RISC). *Depression and Anxiety*. 2003. Vol. 18, № 2. P.76–82.

235. Council of Ministers of the Republic of Bulgaria. Code of Conduct for Civil Servants in the State Administration: Decree No 57, 2 April 2020. *State Gazette*. 2020. No 33(7 April). Режим доступу: https://www.ipa.government.bg/bg/novini/priet-e-nov-kodeks-za-povedenie-na-sluzhitelite (дата звернення: 09.01.2024).

236. Danish business tax affairs. Режим доступу: https://skat.dk/en-us/individuals (дата звернення: 15.08.2025).

237. Department of Finance (Ireland). Circular 09/2009: Civil Servants and Political Activity. 2009. Режим доступу: https://www.gov.ie/en/circular/461b3f526a6446e5a6b15aa6d11d42a2/ (дата звернення 15.08.2025).

238. Department of Finance (Ireland). Civil Service Code of Standards and Behaviour: Circular 26/2004, 9 вересня 2004 р. Режим доступу: https://circulars.gov.ie/pdf/circular/finance/2004/26.pdf (дата звернення: 15.08.2025).

239. Dignum V. The role and challenges of education for responsible AI. *Lond. Rev. Educ*. 2021. Vol. 19. P. 1–11.

240. Dutton W. H. The Oxford Handbook of Internet Studies. – Oxford : Oxford University Press, 2013. Режим доступу: https://doi.org/10.1093/oxfordhb/9780199589074.001.0001 (дата звернення: 15.08.2025).

241. Eke D., Stahl B. Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies // DISO. 2024. Vol. 3, № 11. Режим доступу: https://doi.org/10.1007/s44206-024-00101-6 (дата звернення: 15.06.2025).

242. Erickson John Greenhouse Earth: Tomorrow's Disaster Today. Washington: Tab Books, 1990. 167 p.

243. Estonian Government Office. E-Governance and Digital Communication Policy Guidelines. 2022. Режим доступу: https://www.scribd.com/document/671607084/Estonia-E-Gov-Survey-MSQ-2022 (дата звернення 02.11.2024).

244. Eurofound Hoel H., Di Martino V., Cooper C. L. Preventing violence and harassment in the workplace. Luxembourg : Publications Office of the European Union, 2003. Режим доступу: https://op.europa.eu/en/publication-detail/publication/9920abe9-551d-4719-b926-327bd4b61d5b/language-en (дата звернення 15.08.2025).

245. European Agency for Safety and Health at Work (EU-OSHA). Psychosocial risks and mental health at work. 2022. Режим доступу: https://osha.europa.eu/en/themes/psychosocial-risks-and-stress (дата звернення: 19.01.2025).

246. European Agency for Safety and Health at Work. Digitalisation and workers wellbeing: The impact of digital technologies on work-related psychosocial risks. 2020. Режим доступу: https://osha.europa.eu/en/publications/digitalisation-and-workers-wellbeing-impact-digital-technologies-work-related-psychosocial-risks (дата звернення 12.01.2025).

247. European Commission. The Digital Competence Framework for Citizens (DigComp). Luxembourg : Publications Office of the European Union, 2022. Режим доступу: https://joint-research-centre.ec.europa.eu (дата звернення 17.02.2025).

248. European Commission: Directorate-General for Communications Networks, Content and Technology. Shaping Europe's digital future: Cybersecurity

and Trust. Luxembourg : Publications Office of the European Union, 2020. Режим доступу: https://data.europa.eu/doi/10.2759/091014 (дата звернення 04.05.2025).

249. Eysenck H. J. Manual of the Maudsley Personality Inventory. London, 1959. 247 p.

250. Fang Z. E-Government in digital era: concept, practice, and development. *International Journal of The Computer, The Internet and Management*, Vol. 10, No. 2. 2002. P. 1–22.

251. Floridi L. The Ethics of Information. Oxford : Oxford University Press, 2013. Режим доступу: https://doi.org/10.1093/acprof:oso/9780199641321.001.0001 (дата звернення: 15.08.2025).

252. Gandomi A., Haider M. Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*. 2015. Vol. 35, № 2. P. 137–144.

253. Goleman D. Emotional intelligence: Why it can matter more than IQ. New York : Bantam Books, 2020. Режим доступу: https://archive.org/stream/emotional-intelligence-why-it-can-matter-more-than-iq-daniel-goleman/Emotional%20Intelligence%20Daniel%20Goleman_djvu.txt (дата звернення: 15.08.2025).

254. Gottlieb D. J. Association of Sleep Time With Diabetes Mellitus and Impaired Glucose Tolerance. *Arch Intern Med*. 2005. Vol. 165. No. 8. P. 863–867.

255. Government Communication Service. Digital communication. 2020. Опубліковано 9 березня 2020 р., оновлено 6 листопада 2024 р. Режим доступу: https://gcs.civilservice.gov.uk/guidance/digital-communication/ (дата звернення: 15.08.2025).

256. Government Communication Service. Propriety in digital and social media. 2020. Опубліковано 13 березня 2020 р., оновлено 24 травня 2024 р. Режим доступу: https://gcs.civilservice.gov.uk/guidance/professional-standards/propriety/propriety-in-digital-and-social-media/ (дата звернення: 11.02.2025).

257. Government Communication Service. Social Media Guidance for Civil Servants. 2022. Режим доступу: https://gcs.civilservice.gov.uk/guidance/

professional-standards/propriety/propriety-and-social-media/ (дата звернення 05.04.2025).

258. Government of Canada. Best Practices for Public Servants on Their Personal Use of Social Media. Ottawa : Government of Canada, 2025. Режим доступу: https://www.canada.ca/en/government/publicservice/values/best-practices-public-servants-using-personal-social-media/about-guidance.html (дата звернення 14.12.2024).

259. Government of the United Kingdom. Social media guidance for civil servants: October 2014. Режим доступу: https://www.gov.uk/government/publications/social-media-guidance-for-civil-servants/social-media-guidance-for-civil-servants (дата звернення: 10.06.2025).

260. Graham J., Nosek B. A., Haidt J., Iyer R., Koleva S., Ditto P. H. Mapping the moral domain // Journal of Personality and Social Psychology. 2011. Vol. 101, No 2. P. 366–385.

261. Greening S. G., Mennie K., Lane S. Information technology and its impact on emotional well-being / Lane S. M., Atchley P. (ред.). *Human capacity in the attention economy. Washington : American Psychological Association*/ 2021. P. 49–78.

262. Gross J. J. Emotion regulation: Current status and future prospects // Psychological Inquiry. 2015. Vol. 26, No 1. P. 1–26.

263. Gross J. J., John O. P. Individual differences in two emotion regulation processes: Implications for affect, relationships, and well-being. *Journal of Personality and Social Psychology*. 2003. Vol. 85, No 2. P. 348–362.

264. Hatfield J. M. Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*. 2018. Vol. 73. P. 102–113.

265. Henri L. Critique de la vie quotidienne. T. II. *Fondements d'une sociologie de la quotidienneté*. 1961. Paris, L'Arche. 357 p.

266. Hochreiter S., Schmidhuber, J. Long short-term memory. *Neural Computation*. 1997. Vol. 9 (8). P. 1735–1780.

267. Hogland G., McGraw G. Software Hacking: Code Analysis and

Exploitation. M. : Williams Publishing House, 2005. 400 p.

268. Ince F. Digital Transformation and well-being. *Digital Psychology's Impact on Business and Society. IGI Global*. 2023. 1–27.

269. Indian School of Business Executive Education (ISB ExecEd). Behavioural Insights for Public Sector Leaders. 2023. Режим доступу: https://execed.isb.edu (дата звернення: 15.08.2025).

270. ISO/IEC 27032, Information technology – Security techniques – Guidelines for cybersecurity. 2012. 50 p.

271. Jeffrey L. Elman. Finding structure in time. *Cognitive science*. 1990. Vol. 14(2). P. 179–211.

272. Johns K. Social engineering as a corruption risk // World Bank Governance Blog. 2020. Режим доступу: https://blogs.worldbank.org/en/governance/social-engineering-corruption-risk (дата звернення: 06.07.2025).

273. Joinson A. N., McKenna K. Y. A., Postmes T., Reips U. D. The Oxford Handbook of Internet Psychology. *Oxford : Oxford University Press*, 2009. Режим доступу: https://doi.org/10.1093/oxfordhb/9780199561803.001.0001 (дата звернення 15.08.2025).

274. Kalvet T. Innovation: A factor explaining e-government success in Estonia // Electronic Government, an International Journal. 2012. Vol. 9. № 2. C. 142–157.

275. Kelly G. A. The psychology of personal constructs: Vol. 1. A theory of personality. L.: Routledge. 1991. 422 p.

276. Kowalski R. M., Giumetti G. W., Schroeder A. N., Lattanner M. R. Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*. 2014. Vol. 140, № 4. C. 1073–1137.

277. Kowalski R. M., Limber S. P., McCord A. A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*. 2019. Vol. 45. C. 20–32.

278. Kozup J., Hogarth J. M. Financial literacy, public policy, and consumers' self-protection-More questions, fewer answers. *Journal of Consumer Affairs*. 2008. Vol. 42, № 2. C. 127–136.

279. Lau A. S., Valeri S. M., McCarty C. A., Weisz J. R. Abusive parents' reports of child behavior problems: Relationship to observed parent-child interactions. *Child Abuse & Neglect: journal*. 2006. Vol. 30, no. 6. P. 639–655.

280. Lederer M., Knapp J., Schott, P. The Digital Future Has Many Names: How Business Process Management Drives the Digital Transformation. *Proceedings from: The 6th International Conference on Industry Technology and Management* (ICITM 2017) of IEEE, Cambridge, UK, 7–10 March 2017, P. 22–26.

281. Leroy S. Why is it so hard to do my work? The challenge of attention residue when switching between work tasks // Organizational Behavior and Human Decision Processes. 2009. Vol. 109, № 2. C. 168–181.

282. Leslie D. Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. Zenodo, 2019. Режим доступу: https://doi.org/10.5281/zenodo.3240529 (дата звернення: 11.08.2024).

283. Lim C. Sustainability as Behavioural Change: Nudging the Good, Discouraging the Bad // ETHOS. 2022. Вип. 24 (серпень). Institute of Governance and Policy, Civil Service College. Режим доступу: https://knowledge.csc.gov.sg/ethos-issue-24/sustainability-as-behavioural-change-nudging-the-good-discouraging-the-bad (дата звернення: 27.03.2025).

284. Livingstone S., Stoilova M. The 4Cs: Classifying online risk to children. LSE Research Online, 2021. Режим доступу: https://www.lse.ac.uk (дата звернення: 15.08.2025).

285. Maslach C., Leiter M. P. Burnout. *Stress: Concepts, Cognition, Emotion, and Behavior*. Cambridge : Academic Press, 2016. P. 351–357.

286. Maslach C., Leiter M. P. Understanding burnout / Cooper C. L., Leiter M. P. (ред.). *The handbook of stress and health: A guide to research and practice.*

First Edition. 2017. Режим доступу: https://doi.org/10.1002/9781118993811.ch3 (дата звернення: 15.08.2025).

287. Mendiratta R. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Режим доступу: https://wilmap.stanford.edu/entries/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 (дата звернення: 19.03.2025).

288. Mergel I., Edelmann N., Haug N. Defining digital transformation: Results from expert interviews // Government Information Quarterly. 2019. Vol. 36, No 4. P/ 101–385.

289. Ministry of Finance of Estonia. Code of ethics for officials. Ethics Council of Public Service, 2017. Режим доступу: https://www.fin.ee/en/media/2195/download (дата звернення: 14.04.2025).

290. Ministry of the Interior and Kingdom Relations of the Netherlands. Code of Conduct for the Use of Social Media by Civil Servants. Government of the Netherlands, 2011. Режим доступу: https://www.government.nl/documents/publications/2011/12/01/code-of-conduct-for-the-use-of-social-media-by-civil-servants (дата звернення: 15.08.2025).

291. Moss S., Edmonds B. Sociology and simulation: Statistical and qualitative cross-validation. *American Journal of Sociology*. 2005. VoL. 110, No 4. P. 1095–1131.

292. Mouton F., Nottingham A., Leenen L., Venter H. S. Finite state machine for the social engineering attack detection model: SEADM. *SAIEE Africa Research Journal*. 2018. Vol. 109, No 2. Режим доступу: https://scielo.org.za/scielo.php?pid=S1991-16962018000200004&script=sci_arttext (дата звернення 15.08.2025).

293. Myers D., Twenge J. Social Psychology, 14th Edition, 2022. 440 p.

294. Newcomb T. M. An approach to the study of communicative acts. *Psychol*. Rew., 1953, V. 60, P. 293–304.

295. OECD. Good Practice Principles for Data Ethics in the Public Sector. Paris : OECD Publishing, 2021. Режим доступу: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/03/oecd-good-practice-principles-for-data-

ethics-in-the-public-sector_7a36f20d/caa35b76-en.pdf (дата звернення: 15.08.2025).

296. OECD. OECD Public Integrity Handbook. Paris : OECD Publishing, 2020. Режим доступу: https://doi.org/10.1787/ac8ed8e8-en (дата звернення: 11.07.2025).

297. OECD. Public Employment and Management 2021: The Future of the Public Service. Paris : OECD Publishing, 2021. Режим доступу: https://doi.org/10.1787/938f0d65-en (дата звернення: 15.08.2025).

298. OECD. The OECD Digital Government Policy Framework: Six dimensions of a Digital Government // OECD Public Governance Policy Papers, No 02. Paris : OECD Publishing, 2020. Режим доступу: https://doi.org/10.1787/f64fed2a-en (дата звернення: 15.08.2025).

299. Organisation for Economic Co-operation and Development. The OECD framework for digital talent and skills in the public sector. Paris : OECD Publishing, 2021. Режим доступу: https://doi.org/10.1787/4d7e6c5f-en (дата звернення: 15.08.2025).

300. Paolucci M., Gilbert N., Troitzsch K. G. Simulation for the social scientist. *Journal of Management & Governance*. 2008. No. 12. P. 225–231.

301. Parsons T. D. Ethical challenges in digital psychology and cyberpsychology. Cambridge University Press, 2019. 255 p.

302. Patchin J. W., Hinduja S. Cyberbullying: Identification, prevention, and response. Cyberbullying Research Center, 2020. Режим доступу: https://cyberbullying.org (дата звернення: 15.08.2025).

303. PENSAKI. Case study: How BRFKredit achieved a 90% response rate. 18.02.2021. Режим доступу: https://shop.pensaki.com/en/how-brfkredit-achieved-a-90-percent-response/ (дата звернення: 15.08.2025).

304. Peterson E., Hancock J. T. Digital deception and the future of trust in online environments. *Current Opinion in Psychology*. 2020. Vol. 36. C. 106–110.

305. Pfeiffer S., Bechmann A. Digital maturity and organizational readiness in public administration. Government Information Quarterly. 2022. Vol. 39, No 4. Ст. 101740.

306. Piaget J. The construction of reality in the child. New York: Basic Books. 1954. Режим доступу: http://dx.doi.org/10.1037/11168-000 (дата звернення: 23.02.2024).

307. Rama P., Keevy M. Public cybersecurity awareness good practices on government-led websites. *International Journal of Research in Business and Social Science* (2147-4478). 2023. Vol. 12, No 7. P. 94–104.

308. Raudla R., & Kattel R. Fiscal stress management during the financial and economic crisis: The case of the Baltic countries. *International Journal of Public Administration*. 2013. No 36(10), P. 732–742.

309. Riley T. Electronic Governance: Living and Working in the Wired World. V. 2. 2001. P. 49-66.

310. Robinson N. D. Systems of Modern Psychology. Columbia University Press, New York, 1979. 323 p.

311. Rogers C. On Becoming a Person: A Therapist's View of Psychotherapy. Mariner Books, 1961. 400 p.

312. Rogers C. R. A Theory of Therapy, Personality, and Interpersonal Relationships: As Developed in the Client-Centered Framework. In S. *Koch (Ed.), Psychology: A Study of a Science. Formulations of the Person and the Social Context New York: McGraw Hill*. 1959. Vol. 3. pp. 184–256.

313. Rousseau D. Психологічні контракти в організаціях: розуміння письмових і неписьмових угод. *SAGE Publications Inc*., 1995. DOI: https://doi.org/10.4135/9781452231594

314. Rumelhart D. E., Hinton G. E., Williams R. J. Learning internal representations by error propagation. *In Parallel distributed processing: Explorations in the microstructure of cognition.* MIT Press. 1986. Vol. 1. P. 318–362.

315. Rydnik V. ABC's of quantum Mechanics. M. : Mir Publishers, 1978 p.

316. Ryen White; Eric Horvitz. Cyberchondria: Studies of the escalation of medical concerns in Web search. *ACM Transactions on Information Systems*. 2009. No 27(4). P. 1–37.

317. SAGE Journals. Ethical Persuasion and Behavioural Public Policy 2021. Режим доступу: https://journals.sagepub.com/

318. Service O., Hallsworth M., Halpern D., Algate F., Gallagher R., Nguyen S., Ruda S., Sanders M. EAST: Four simple ways to apply behavioural insights – The Behavioural Insights Team/ 2014. Режим доступу: https://www.bi.team/publications/east-four-simple-ways-to-apply-behavioural-insights/

319. Sharma M., Pendyal K. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Protection from Malicious Content or Chilling Free Speech 1 листопада 2021. Режим доступу: https://ssrn.com/abstract=3967857

320. Shevchenko A. Digital era. Just about digital technology. Kyiv: Summit Book, 2018. 457 p.

321. Shevchenko S. V., Falko, N. M. Rozvytok komunikatyvnoi kompetentnosti maibutnikh psykholohiv. *Development of communicative competence of future psychologists*. Habitus, 2020. No 2(18). P. 143–148.

322. Smith A. Handbook of Human Performance. London: Acad. Press, 1992. 340 p.

323. Thaler R. H., Sunstein C. R. Nudge: Improving Decisions About Health, Wealth, and Happiness Yale University Press, 2008. Режим доступу: https://www.researchgate.net/publication/257178709_Nudge_Improving_Decisions_About_Health_Wealth_and_Happiness_RH_Thaler_CR_Sunstein_Yale_University_Press_New_Haven_2008_293_pp

324. The Gazette Of India: Extraordinary. Ministry of Electronics and Information Technology. Notification – New Delhi, 25 лютого 2021. PART II-SEC. 3(i). P. 19-34. Режим доступу: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

325. The GovLab. MindLab: The evolution of a public innovation lab – 7 березня 2016. Режим доступу: https://blog.thegovlab.org/mindlab-the-evolution-of-a-public-innovation-lab

326. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 Updated as on 6.4.2023. Режим доступу: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

327. The Ministry of Manpower. Committee of Supply 2024: Foreign Workforce Policy Announcements 4 березня 2024. Режим доступу: https://www.mom.gov.sg/newsroom/press-releases/2024/cos-foreign-workforce-policy-factsheet

328. Toews D. «The New Tarde: Sociology after the End of the Social». Theory Culture & Society, 2003. Vol. 20. No. 5. P. 81–98.

329. UK Civil Service Learning. Digital and data capability UK Government, 2021. Режим доступу: https://www.gov.uk/government/organisations/civil-service

330. Vazquez-Venegas P. та ін. Digital and innovative tools for better health and productivity at the workplace OECD Health Working Papers, No. 169, OECD Publishing, Paris, 2024. Режим доступу: https://doi.org/10.1787/2ce05eb6-en

331. Verizon. 2022 Data Breach Investigations Report. Verizon Enterprise, 2022. Режим доступу: https://www.verizon.com/business/resources/reports/dbir

332. Vogels E. A. The state of online harassment. *Pew Research Center*. 2021. Режим доступу: https://www.pewresearch.org

333. Vuorikari R., Kluzer S., Punie Y. DigComp 2.2: The Digital Competence Framework for Citizens. *Publications Office of the European Union*. Luxembourg, 2022. doi:10.2760/115376

334. Watson J. B. Psychology as the behaviorist views it. *Psychological Review*, 1913. Vol. 20 (2), 158–177.

335. Whitty M. T. Cyberpsychology: The Study of Individuals, Society and Digital Technologies. / Monica T. Whitty. Editor Garry Young. John Wiley & Sons, 2016. 272 p.

336. Wilbur L., Higley M., Hatfield J., Surprenant Z., Taliaferro E., Smith D., Paolo A. Survey results of women who have been strangled while in an abusive relationship. *The Journal of Emergency Medicine*. 2001. Vol. 21, no. 3. P. 297–302.

337. Yates David M. (1997). Turing's Legacy: A History of Computing at the National Physical Laboratory 1945-1995 (англ.). National Museum of Science and Industry. Архів оригіналу за 3 серпня 2020.

338. Vasylieva, N., Boiko, O., Vasylieva, O., Dubkov, A., & Chubina, A. (2024). Plataforma electrónica para las consultas de las autoridades públicas a los residentes de las comunidades en el contexto de la descentralización. Boletín Mexicano De Derecho Comparado, 1(166), 27-47.

339. Андріяш В., Архипова Н. Кадровий потенціал організації: понятійно-змістовий аналіз. *Державне управління: удосконалення та розвиток*. № 9. 2025. URL: https://www.nayka.com.ua/index.php/dy/article/view/7510

340. Васильєва Н., Васильєва О., Приліпко С. Професійне становлення службовців органів публічної влади: сучасні виклики. *Публічне управління та регіональний розвиток*. 2024. № 23. С. 107-122. URL: https://pard.mk.ua/index.php/journal/article/view/406

341. Васильєва О.В. Збереження ментального здоров'я державних службовців – важливе завдання служб управління персоналом. *Наукові перспективи* . 2025. № 9(63). С. 45-54 URL:https://perspectives.pp.ua/index.php/np/article/view/29489

342. Івашова Л. М., Бондаренко Л. І. Інституційні зміни змісту й організації діяльності органів виконавчої влади в умовах інноваційних трансформацій в Україні: монографія. Дніпро: УМСФ, 2025. 155 с.

343. Івашова Л.М., Бондаренко Л.І. Аналіз стану інституційної реформи державного управління й її наслідків за змістовно-функціональним

та організаційним критеріями // Публічне управління та митне адміністрування. 2023. №1 (36). С.17-41. URL: http://customs-admin.umsf.in.ua/archive/2023/1/5.pdf

344. Івашова Л.М., Івашов М.Ф., Шевченко Н.І. Професіоналізація як інструмент управління персоналом публічної служби // Публічне управління та митне адміністрування. 2021. №4 (31). С.52-58. URL: http://www.customs-admin.umsf.in.ua/archive/2021/4/10.pdf

345. Тодорова М., Штиров О. Роль поведінкових теорій у процесі аналізу мотивів кібернетингу в публічному просторі. *Державне управління та регіональний розвиток* . 2025. №29. С. 997–1024. URL: https://pard.mk.ua/index.php/journal/article/view/544

346. Штирьов О. М., Жовнірчик Я. Ф., Сухорукова А. Л. Управління персоналом як інструмент формування антикорупційних механізмів у системі державної служби. *Інвестиції: практика та досвід.* 2025. № 18. С. 212-219 URL: https://www.nayka.com.ua/index.php/investplan/article/view/7491/7617

347. Штирьов О. М., Жовнірчик Я. Ф., Антонова Л.В. Роль процесу управління персоналом у розвитку державної служби країн ЄС *Державне управління: удосконалення та розвиток*. 2025. № 10. URL: https://www.nayka.com.ua/index.php/dy/article/view/7757/7887

348. Шульга А.А., Сергієнко В.М. Оптимізація системи управління персоналом на державній службі в контексті розвитку інформаційного суспільства. *Інвестиції: практика та досвід.* 2025. № 18. С. 260-267. URL: https://nayka.com.ua/index.php/investplan/article/view/7498/7624

349. Шульга А.А., Сергієнко В.М. Правові засади управління персоналом на державній службі в умовах розвитку інформаційного суспільства. *Публічне управління та регіональний розвиток*. 2025, № 29. С. 895-928.

ДОДАТОК А

Таблиця 1

Концептуальні засади існування особистості в кіберпросторі: аналіз і порівняння психологічних теорій та теорій нейромереж

Автори наукових шкіл, теорій, концепцій	Ключові положення теорій	Примітки
Теорія особистісних конструктів Дж. Келлі [272]	…особистість формується через інтерпретацію та обробку інформації, що надходить із зовнішнього середовища внутрішніми нейронними мережами. Кожна особистість має свої унікальні нейронні мережі, які формують основу для створення її «профілю» – особистісних конструктів.	Базуючись на ідеї унікальних особистісних конструктів кожної людини, цифрові платформи можуть створювати персоналізовані рекомендації для користувачів, враховуючи їхні індивідуальні потреби та вподобання, інтерактивні технології – для створення особистісних тестів. У галузі досліджень веб-сайтів та додатків ця теорія може бути використана для аналізу та прогнозування індивідуальних реакцій користувачів на різні інтеракційні дизайни.
Психоаналітична теорія З. Фрейда [196]	…відзначається акцентом на несвідомих мотивах, конфліктах і пригнічених бажаннях, які впливають на формування особистості.	У сучасному цифровому світі контакт з технологіями (соцмережі, віртуальна реальність та інше) може відображати індивідуальні прагнення користувачів та їх конфлікти. В умовах віртуальної реальності можуть виникати процеси, аналогічні роботі безсвідомого, коли реакції на подразники відбуваються без свідомого контролю. Віртуальний простір – це широке поле для анонімних проявів усіх витіснених бажань та агресивних імпульсів. Хейтинг, троллінг, флеймінг, доксінг, сталкінг, кібербулінг, ігри з насильством – усе це прояви деструктивного начала людини, так званого Танатоса.
Гуманістична психологія (А. Маслоу, К. Роджерс та ін.) [311; 312]	…самоактуалізація є процесом реалізації власного потенціалу та прагнення до власного вдосконалення, який спонукає людину до пошуку нових знань, досягнень і розвитку. Підкреслюється важливість суб'єктивного досвіду кожної особистості, вважаючи, що саме індивідуальний підхід та розуміння внутрішніх переживань можуть допомогти людині досягти гармонії та задоволення у житті.	З огляду на гуманістичну психологію, цифрові технології можуть бути використані для створення платформ та додатків, які сприяють саморозвитку, підвищенню самосвідомості та самоприйняття. Також може бути корисним для створення емпатичного та підтримуючого середовища, інтуїтивно зрозумілих та дружніх до користувача інтерфейсів.

Продовження табл. 1

Біхевіоризм (Дж.Уотсон, Ф. Скіннер та ін.) [334]	…обґрунтовує вивчення поведінки людини через зовнішні подразники та реакції на них. Дана концепція полягала в тому, що поведінка може бути керована за допомогою відповідного стимулювання та посилення важливих досліднику аспектів. Таким чином, підкріплення, яке збільшує бажану поведінку, та покарання, яке, навпаки, зменшує, виступають як ключові інструменти оперантного обумовлення	Біхевіоризм впливає на методи навчання та вирішення завдань у віртуальних навчальних середовищах, де використання позитивного підкріплення, такого як навчальні бейджі, віртуальні нагороди та рівні, може стимулювати вивчення та досягнення результатів. Системи штучного інтелекту та аналітики даних можуть використовувати принципи біхевіоризму для аналізу та вдосконалення підходів до навчання та викладання. В інтернет-терапії та додатках для психологічної підтримки можна застосовувати принципи біхевіоризму для створення програм, які сприяють позитивній зміні поведінки та звичок.
Когнітивна психологія (Ж. Піаже, Л. Виготський та ін.) [306]	…описує процес когнітивного розвитку як послідовність стадій, кожна з яких характеризується якісними змінами у способі мислення, розуміння світу та розв'язанні людиною проблем. розвинув концепцію культурно-історичного підходу до розуміння когнітивних процесів. За цією концепцією, розвиток людського мислення нерозривно пов'язаний з соціальними та культурними впливами, що оточують індивіда.	Когнітивна психологія має безліч застосувань у сучасному цифровому світі, особливо в контексті розвитку технологій. Це і дизайн інтуїтивно зрозумілих та ефективних інтерфейсів для програм та вебсайтів, і розробка програм навчання та тренажерів, які сприяють кращому засвоєнню матеріалу та розвитку навичок, і розвиток та покращення алгоритмів штучного інтелекту, зокрема в галузях комп'ютерного зору, мовленнєвого процесу та автономної навігації, і розробка цифрових психологічних тестів та оцінювальних інструментів на основі принципів когнітивної психології для діагностики та дослідження рівня когнітивних функцій особистості, а також використання когнітивних принципів для створення іммерсивних інтерактивних дослідницьких середовищ та ігор у віртуальній реальності.
Теорія соціального пізнання А. Бандури [218]	…людина навчається не лише через власний досвід, але й шляхом спостереження за іншими та моделювання їхньої поведінки; соціальне навчання впливає на формування певних психологічних процесів та вмінь у людини, зокрема на формування уявлень про себе, віру у власні можливості та стиль вирішення конфліктів.	Враховуючи, що велика частина спілкування відбувається онлайн, ця теорія допомагає визначити, як взаємодія з іншими користувачами та спостереження за їхньою поведінкою впливає на формування уявлень про себе та розвиток особистості. Також ця теорія може бути застосована в розвитку цифрових платформ для навчання та розвитку особистості, де спостереження та моделювання поведінки може бути використано для покращення процесу навчання та розвитку навичок.

Продовження табл. 1

Теорія рис Р. Кеттелла [231]	…концепція «трейтів» (рис) представляє собою стійкі якості поведінки, які проявляються у різних ситуаціях та є відносно стійкими в часі. За цією теорією, особистість складається з певного набору трейтів, кожен з яких може бути виміряний та класифікований. Трейти допомагають розуміти, чому люди ведуть себе по-різному в різних ситуаціях і чому їхня поведінка може залишатися стійкою впродовж тривалого часу.	Враховуючи, що велика частина взаємодії відбувається через інтернет, зрозуміння трейтів користувачів може допомогти в покращенні персоналізації середовища та підвищенні ефективності комунікації. Також ця теорія може бути застосована в розвитку алгоритмів машинного навчання для створення більш точних моделей користувачів та удосконалення систем рекомендацій і персоналізованих послуг.
Психологічна теорія особистості Г. Айзенка [249]	…параметри нервової системи, такі як сила збудження та гальмування, мають визначальний вплив на формування особистості через три ключові фактори: екстраверсія-інтроверсія, нейротизм-стабільність, психотизм.	Ця теорія може бути корисною для розуміння та аналізу користувачів в онлайн-середовищах, також може допомогти розробляти більш ефективні та персоналізовані підходи до взаємодії з користувачами, зокрема, у сфері маркетингу, дизайну інтерфейсів та рекомендаційних систем.

Таблиця 2

Додатки і технології, що розроблені на основі нейромереж

№ з/п	Назви технологій	Особливості застосування
1.	Нейротренажери (brain training apps)	Наприклад, додатки Lumosity, Peak і Elevate використовують ігри та вправи на основі нейронних мереж для покращення пам'яті, уваги, швидкості мислення та інших когнітивних функцій.
2.	Пристрої для нейромодуляції (neurostimulation devices)	Серед них можна виділити технології, які називаються tDCS (транскраніальне постійне електричне збудження) та TMS (транскраніальна магнітна стимуляція), що використовуються для стимулювання конкретних ділянок головного мозку з метою покращення когнітивних здібностей, таких як збільшення уваги та концентрації.
3.	Персоналізовані освітні платформи (personalized learning platforms)	Деякі платформи, такі як Duolingo для вивчення іноземних мов або Coursera для онлайн-навчання, використовують алгоритми машинного навчання та нейронні мережі для створення персоналізованих курсів і вправ з метою покращення когнітивних здібностей.
4.	Інтерфейси мозок-комп'ютер (brain-computer interfaces)	Ці технології дозволяють управляти пристроями та застосунками за допомогою думок. Наприклад, EEG-інтерфейси використовують нейронні мережі для обробки та інтерпретації електричної активності мозку з метою покращення когнітивних здібностей людини.
5.	Програмне забезпечення для розпізнавання емоцій (emotion recognition software)	Нейронні мережі можуть використовуватися для створення програмного забезпечення, яке розпізнає емоції за виразом обличчя, інтонацією голосу та іншими ознаками. Це сприяє покращенню навичок сприйняття та розуміння людьми емоцій.
6.	Когнітивні асистенти (cognitive assistants)	Системи, такі як Google Assistant або Apple's Siri, використовують нейронні мережі для поліпшення взаємодії з користувачем, надаючи персоналізовані рекомендації та допомогу у виконанні повсякденних завдань.
7.	Когнітивне тренування у віртуальній реальності (virtual reality cognitive training)	Технології віртуальної реальності з використанням нейронних мереж створюють середовище для покращення когнітивних функцій, як-от пам'ять, увага і координація, через інтерактивні та іммерсивні тренування.
8.	Пристрої для моніторингу мозкової активності (brainwave monitoring devices)	Нейрогарнітури Muse Headband або NeuroSky MindWave, моніторять електричну активність мозку та використовують нейронні мережі для аналізу даних, що допомагає покращити концентрацію та стрес-менеджмент.

ДОДАТОК Б

Опитувальник (Анкета)

Шановні учасники!

Дякуємо Вам за готовність взяти участь у цьому дослідженні, присвяченому питанням безпечного цифрового середовища для державних службовців України.

Метою опитування є вивчення Вашого досвіду перебування у цифровому просторі, зокрема пов'язаного з такими викликами, як кіберхейт. Отримані результати допоможуть розробити ефективні заходи підтримки та сприятимуть формуванню безпечного й доброзичливого Інтернету для всіх користувачів.

Опитування є анонімним. Всі Ваші відповіді будуть використані виключно в наукових цілях і оброблятимуться конфіденційно. Будь ласка, відповідайте чесно. Пам'ятайте, що правильних чи неправильних відповідей не існує, а участь є добровільною.

Дякуємо за Ваш внесок у створення безпечного цифрового середовища.

Інформація про мене

1. До якої статі Ви себе відносите?

- чоловіча
- жіноча
- інше

2. Скільки Вам років? _____

3. Якою мовою Ви розмовляєте вдома? _____

4. Що з переліченого найкраще описує район, де Ви живете?

- **Місто** – щільно заселений район, де зазвичай добре розвинена інфраструктура, така як дороги та будівлі, з високим рівнем забруднення та швидким темпом життя.
- **Передмістя** – місцевість, що оточує місто, часто з поєднанням житлових і промислових районів, іноді менш щільно заселена, ніж місто, але щільніше заселена, ніж сільська місцевість.
- **Сільська місцевість** – малонаселена місцевість, де можуть бути великі відкриті простори, сільськогосподарські ділянки та невеликі поселення. Життя у сільській місцевості часто сприймається як повільніше проти міського.

5. Чи належить місто, з якого Ви родом, до гарячої точки?

- Так
- Ні

6. У якому місті Ви живете тепер?_____

7. Визначте, наскільки Ви згодні або не згодні з наведеними твердженнями:

1.	Загалом я задоволений(на) собою	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
2.	Іноді я думаю, що я у всьому поганий(на)	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
3.	Мені здається, що в мене є низка хороших якостей	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
4.	Я здатний дещо робити не гірше, ніж більшість	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
5.	Мені здається, що мені особливо немає чим пишатися	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
6.	Іноді я відчуваю свою неефективність	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
7.	Я відчуваю, що я гідна людина, принаймні не менше за інших	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
8.	Мені хотілося б більше поважати себе	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
9.	Я завжди схильний/схильна почуватися невдахою	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
10.	Я до себе добре ставлюся	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
11.	Я дуже скептична людина і ставлюся до всього з обережністю та увагою	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)

8. Будь ласка, вкажіть нижче, наскільки добре у Вас налагоджено спілкування з колегами:

1.	Я можу обговорювати свої погляди з кимось із колег, не відчуваючи при цьому скутості чи збентеження	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
2.	Мої колеги завжди уважно слухають мене	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
3.	Я дуже задоволений тим, як ми з колегами спілкуємося	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
4.	Якби в мене були неприємності, я міг би розповісти про це колегам	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)

9. Наскільки Ви довіряєте наступним установам чи особам?

1.	Президент	о я не довіряю	о я не впевнений(на)	о я трохи довіряю	о я дуже довіряю
2.	Мій керівник/моє керівництво	о я не довіряю	о я не впевнений(на)	о я трохи довіряю	о я дуже довіряю
3.	Політики	о я не довіряю	о я не впевнений(на)	о я трохи довіряю	о я дуже довіряю
4.	Мої колеги	о я не довіряю	о я не впевнений(на)	о я трохи довіряю	о я дуже довіряю
5.	Поліція	о я не довіряю	о я не впевнений(на)	о я трохи довіряю	о я дуже довіряю
6.	Закон/правова система	о я не довіряю	о я не впевнений(на)	о я трохи довіряю	о я дуже довіряю
7.	Засоби масової інформації	о я не довіряю	о я не впевнений(на)	о я трохи довіряю	о я дуже довіряю

Користування інтернетом

10. Скільки часу Ви проводите в Інтернеті в робочий час?

- До 30 хвилин
- 1-3 години
- 3-5 годин
- Більше 5 годин

11. Як часто під час виконання службових обов'язків Ви відволікаєтеся на неслужбові онлайн-активності (наприклад, перегляд соціальних мереж, особисті листування, перегляд розважального контенту)?

- ніколи
- рідко (раз на тиждень або рідше)
- іноді (декілька разів на тиждень)
- часто (щодня або майже щодня)
- постійно (протягом більшої частини робочого дня)

12. Як часто Ви відкладаєте виконання робочих завдань або прийняття рішень, переключаючись на менш важливі або незначущі онлайн-активності (наприклад, читання новин, перевірка соцмереж, перегляд відео)?

- ніколи
- рідко (раз на тиждень або рідше)
- іноді (декілька разів на тиждень)
- часто (щодня або майже щодня)
- дуже часто (це відбувається постійно)

13.Як часто ці речі відбувалися з Вами за останній рік?

1	Я не їв(ла) і не спав(ла) через Інтернет	o Ніколи	o Кілька разів	o Принаймні щотижня	o Щодня або майже щодня
2	Я відчував(ла) роздратування, коли не міг(могла) зайти в Інтернет	o Ніколи	o Кілька разів	o Принаймні щотижня	o Щодня або майже щодня
3	Я виявив(ла), що користуюся Інтернетом, навіть якщо він мене не дуже цікавить	o Ніколи	o Кілька разів	o Принаймні щотижня	o Щодня або майже щодня
4	Через час, проведений в Інтернеті, я приділяю менше часу сім'ї, друзям чи роботі, ніж варто було б	o Ніколи	o Кілька разів	o Принаймні щотижня	o Щодня або майже щодня
5	Я безуспішно намагався(лася) проводити менше часу в Інтернеті	o Ніколи	o Кілька разів	o Принаймні щотижня	o Щодня або майже щодня

Користування соціальними мережами: кіберхейт.

Наступні питання стосуються теми кіберхейту. ***Кіберхейт*** *– це явище, коли хтось навмисно пише чи ділиться в інтернеті злісними чи ненависними коментарями про інших людей. Це може відбуватися у соціальних мережах, на форумах або за допомогою повідомлень. Йдеться про слова або зображення, які принижують людину через її походження, зовнішність, погляди або ще щось, що визначає її.*

14. Як часто Ви користуєтеся наведеними нижче соціальними мережами?

1	Tik-Tok	o ніколи	o менше 2 годин на день	o 2-4 години на день	o більше 4 годин на день
2	Twitch	o ніколи	o менше 2 годин на день	o 2-4 години на день	o більше 4 годин на день
3	YouTube	o ніколи	o менше 2 годин на день	o 2-4 години на день	o більше 4 годин на день
4	Online Messenger: WhatsApp, Telegram, Signal	o ніколи	o менше 2 годин на день	o 2-4 години на день	o більше 4 годин на день
5	Twitter / X	o ніколи	o менше 2 годин на день	o 2-4 години на день	o більше 4 годин на день
6	Instagram	o ніколи	o менше 2 годин на день	o 2-4 години на день	o більше 4 годин на день
7	Facebook	o ніколи	o менше 2 годин на день	o 2-4 години на день	o більше 4 годин на день
8	Discord	o ніколи	o менше 2 годин на день	o 2-4 години на день	o більше 4 годин на день
9	Viber				

15.Чи маєте відчуття, що за останні 12 місяців кількість кіберхейту збільшилася?

- Так
- Ні

16. На яких платформах і як часто Ви спостерігали кіберхейт:

1	Tik-Tok	о ніколи	о рідко	о періодично	о часто	о не користуюся цією платформою
2	Twitch	о ніколи	о рідко	о періодично	о часто	о не користуюся цією платформою
3	YouTube	о ніколи	о рідко	о періодично	о часто	о не користуюся цією платформою
4	Online Messenger: WhatsApp, Telegram, Signal	о ніколи	о рідко	о періодично	о часто	о не користуюся цією платформою
5	Twitter / X	о ніколи	о рідко	о періодично	о часто	о не користуюся цією платформою
6	Instagram	о ніколи	о рідко	о періодично	о часто	о не користуюся цією платформою
7	Facebook	о ніколи	о рідко	о періодично	о часто	о не користуюся цією платформою
8	Discord	о ніколи	о рідко	о періодично	о часто	о не користуюся цією платформою
9	Viber	о ніколи	о рідко	о періодично	о часто	о не користуюся цією платформою

17. На Вашу думку, де найчастіше трапляється ненависть?

1	Образливі пости чи відеоролики у соціальних мережах чи інших інтернет-сайтах	о ніколи	о рідко	о періодично	о часто	о не знаю
2	Коментарі з образливим змістом у соціальних мережах, на веб-сайтах, форумах чи блогах	о ніколи	о рідко	о періодично	о часто	о не знаю
3	Групові чати (робочі, батьківські та ін.) (наприклад, у Viber, WhatsApp, Telegram та ін.)	о ніколи	о рідко	о періодично	о часто	о не знаю
4	Особисті повідомлення	о ніколи	о рідко	о періодично	о часто	о не знаю
5	Онлайн ігри	о ніколи	о рідко	о періодично	о часто	о не знаю

18. За якими темами Ви спостерігали кіберхейт у соціальних мережах за останні 12 місяців?

1	Гомосексуальність чи сексуальність загалом. Це може включати думки або заяви про відносини між людьми, їх сексуальну орієнтацію або поведінку	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
2	Розмір людини (худа або повна статура)	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
3	Люди з іншим кольором шкіри	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
4	Люди з певними політичними поглядами	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю

5	Тема політики/ політичні діячі	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
6	Люди з обмеженими можливостями здоров'я	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
7	Достаток людини (бідні чи багаті люди)	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
8	Люди інших культур та національностей	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
9	Біженці чи переселенці	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
10	Висловлювання та зміст, пов'язані з приналежністю до певної релігії	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
11	Вік	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю
12	Жінки	о ніколи	о кілька разів	о принаймні щомісяця	о частіше	о не знаю

20. Які емоції викликає у Вас загальне сприйняття ненависті в Інтернеті?

1	У мене з'являється бажання протистояти цьому	о ніколи	о рідко	о періодично	о часто	о не знаю
2	Я почуваюся безпорадним(ною)	о ніколи	о рідко	о періодично	о часто	о не знаю
3	Мені все одно	о ніколи	о рідко	о періодично	о часто	о не знаю
4	Мені подобається спостерігати за цим/ мені смішно бачити ненависть в Інтернеті	о ніколи	о рідко	о періодично	о часто	о не знаю
5	Я намагаюся забути про це	о ніколи	о рідко	о періодично	о часто	о не знаю
6	Я злюсь через це	о ніколи	о рідко	о періодично	о часто	о не знаю
7	Я засмучуюсь через це	о ніколи	о рідко	о періодично	о часто	о не знаю
8	Я відчуваю, що моя думка збігається з цими висловлюваннями	о ніколи	о рідко	о періодично	о часто	о не знаю
9	Мене це розважає	о ніколи	о рідко	о періодично	о часто	о не знаю
10	З'являється бажання помститися цій людині	о ніколи	о рідко	о періодично	о часто	о не знаю

21. Як Ви справляєтеся з ненавистю в Інтернеті загалом?

1	Ніяк, не реагую	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
2	Я закриваю сайт або програму	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
3	На деякий час я перестаю користуватися Інтернетом	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
4	Я обговорюю це зі своїми друзями	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
5	Я розповідаю про це своїм колегам	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
6	Я відповідаю і вступаю в конфронтацію з людиною	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
7	Я говорю про це зі своїм керівником	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
8	Я повідомляю про цей випадок у поліцію	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
9	Я коригую/міняю свої налаштування конфіденційності	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
10	Я повідомляю платформу про те, що певний контент або	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)

облікові записи, про які я знаю, можуть бути токсичними, щоб його можна було видалити чи заблокувати

11 Я використовую функції блокування та сповіщення, коли стикаюся з ненавистю в Інтернеті — о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)

22. Чи стикалися Ви протягом останніх 12 місяців з негативними висловлюваннями в Інтернеті на адресу себе чи групи, до якої Ви належите (наприклад, з приводу Вашої релігії, політичних поглядів чи сексуальної орієнтації, мови чи національної приналежності)? Це може означати, що хтось грубив Вам в мережі або говорив речі, які зачіпали Вас чи таких самих людей, як і Ви.

1. у коментарях — о ніколи о рідко о іноді о часто о не знаю
2. у постах або на відео у соціальних мережах — о ніколи о рідко о іноді о часто о не знаю
3. у групових чатах — о ніколи о рідко о іноді о часто о не знаю
4. в особистих повідомленнях — о ніколи о рідко о іноді о часто о не знаю

23. Чи траплялося з Вами щось із перерахованого за останні 12 місяців?

1 Мені надсилали злі чи образливі повідомлення — о ніколи о рідко о періодично о часто о не знаю
2 Про мене розсилали злі чи образливі повідомлення, щоб інші могли їх побачити — о ніколи о рідко о періодично о часто о не знаю
3 В Інтернеті мені погрожували, шантажували, чинили на мене тиск — о ніколи о рідко о періодично о часто о не знаю
4 Мені надходили повідомлення сексуального змісту, хоча я цього не хотів(ла) — о ніколи о рідко о періодично о часто о не знаю
5 Було опубліковано мої особисті чи ганебні фотографії — о ніколи о рідко о періодично о часто о не знаю

24. За останні 12 місяців Ви стикалися з проявами ненависті в Інтернеті щодо людей, яких Ви знаєте особисто, наприклад, друзів, членів сім'ї, колег або керівництва (наприклад, за релігійними, мовними/національними приналежностями або політичними переконаннями, сексуальною орієнтацією, тощо).

1. У коментарях — о ніколи о рідко о іноді о часто о не знаю
2. У постах або на відео у соціальних мережах — о ніколи о рідко о іноді о часто о не знаю
3. У групових чатах — о ніколи о рідко о іноді о часто о не знаю
4. В особистих повідомленнях — о ніколи о рідко о іноді о часто о не знаю

25. Які емоції Ви відчували, коли бачили ненависть в Інтернеті до Вас або до людей з Вашого особистого оточення?

1	У мене з'являється бажання протистояти цьому	о ніколи	о рідко	о періодично	о часто	о не знаю
2	Я почуваюся безпорадним(ною)	о ніколи	о рідко	о періодично	о часто	о не знаю
3	Мені все одно	о ніколи	о рідко	о періодично	о часто	о не знаю
4	Мені подобається спостерігати за цим/ мені смішно бачити ненависть в Інтернеті	о ніколи	о рідко	о періодично	о часто	о не знаю
5	Я намагаюся забути про це	о ніколи	о рідко	о періодично	о часто	о не знаю
6	Я злюсь через це	о ніколи	о рідко	о періодично	о часто	о не знаю
7	Я засмучуюсь через це	о ніколи	о рідко	о періодично	о часто	о не знаю
8	Я відчуваю, що моя думка збігається з цими висловлюваннями	о ніколи	о рідко	о періодично	о часто	о не знаю
9	З'являється бажання помститися цій людині	о ніколи	о рідко	о періодично	о часто	о не знаю

26. Як Ви справляєтеся з ненавистю в Інтернеті щодо Вас чи людей із Вашого особистого оточення?

1	Ніяк, не реагую	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
2	Я говорю на цю тему з друзями	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
3	Я говорю на цю тему з колегами	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
4	Я відповідаю і вступаю у конфронтацію з людиною	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
5	Я говорю на цю тему з керівництвом	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
6	Я повідомляю про цей випадок у поліцію	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
7	Я коригую свої налаштування конфіденційності	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
8	Я повідомляю платформу про те, що певний контент або облікові записи, про які я знаю, можуть бути токсичними, щоб його можна було видалити чи заблокувати	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)
9	Я використовую функції блокування та сповіщення, коли стикаюся з ненавистю в Інтернеті	о абсолютно не згоден(дна)	о не згоден(дна)	о важко відповісти	о згоден(дна)	о повністю згоден(дна)

27. За останні 12 місяців Ви коли-небудь ділилися або говорили в Інтернеті щось, що могло б образити інших? (Наприклад, щось грубе, особисте чи залякуюче, чи спрямоване на людей іншої національності, місця, звідки вони родом, їхньої релігії, того, хто вони – чоловік чи жінка, чи хто їм подобається).

- ніколи
- рідко
- періодично
- часто
- не знаю

28. Протягом останніх 12 місяців, якщо Ви поділилися або сказали в Інтернеті щось, що могло образити інших людей (наприклад, щось грубе, особисте чи залякуюче або спрямоване проти людей через кольор їхньої шкіри, національність, місця, звідки вони родом, їхньої релігії, того, хто вони – чоловік чи жінка, або хто їм подобається), яка була тому причина?

1	Тому що ця людина заслужила на це	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)
2	Тому що у мене неприємності з цією людиною	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)
3	Тому що ця людина також сказала або поділилася чимось неприємним щодо мене	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)
4	Просто заради забави / думаю це смішно	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)
5	Щоб помститися за інших, яких образили	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)
6	Тому що мені нудно	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)
7	Тому що в мене був поганий настрій	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)
8	Тому що інші теж так роблять	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)
9	Тому що це круто	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)
10	Тому що я хочу висловити свою думку	о абсолютно не згоден(дна) о не згоден(дна) о важко відповісти о згоден(дна) о повністю згоден(дна)

Довірча особа та тематизація ненависті в Інтернеті

29. Коли в останній раз в Інтернеті сталося щось, що Вас засмутило, Ви говорили про це з кимось із перелічених людей чи організацій?

1	Члени сім'ї / родичі	o абсолютно не згоден(дна) o повністю згоден(дна)	o не згоден(дна)	o важко відповісти	o згоден(дна)
2	Друг/подруга	o абсолютно не згоден(дна) o повністю згоден(дна)	o не згоден(дна)	o важко відповісти	o згоден(дна)
3	Колеги	o абсолютно не згоден(дна) o повністю згоден(дна)	o не згоден(дна)	o важко відповісти	o згоден(дна)
4	Керівництво	o абсолютно не згоден(дна) o повністю згоден(дна)	o не згоден(дна)	o важко відповісти	o згоден(дна)
5	Терапевт / психолог / лікар	o абсолютно не згоден(дна) o повністю згоден(дна)	o не згоден(дна)	o важко відповісти	o згоден(дна)
6	Поліція	o абсолютно не згоден(дна) o повністю згоден(дна)	o не згоден(дна)	o важко відповісти	o згоден(дна)
7	Онлайн-портал допомоги та довіри	o абсолютно не згоден(дна) o повністю згоден(дна)	o не згоден(дна)	o важко відповісти	o згоден(дна)
8	Психологічні консультаційні центри / Телефон довіри	o абсолютно не згоден(дна) o повністю згоден(дна)	o не згоден(дна)	o важко відповісти	o згоден(дна)
9	Ніхто	o абсолютно не згоден(дна) o повністю згоден(дна)	o не згоден(дна)	o важко відповісти	o згоден(дна)

30. Яку підтримку Ви хотіли б отримати, якби зіткнулися з ненавистю в Інтернеті? (можливі кілька відповідей)

- Емоційна підтримка (наприклад, хтось, з ким можна поговорити)
- Юридична консультація (інформація про мої права та можливі дії)
- Технічна допомога (наприклад, блокування або повідомлення про користувачів)
- Освітні ресурси (щоб краще зрозуміти, що таке кіберзалякування/ненависть і як з ними боротися)
- Додаткові тренінги/семінари з цієї теми
- Підтримка не потрібна

31. Чи розглядалася тема ненависті в Інтернеті у Вашому робочому просторі?

- Ця тема обговорювалася під час підвищення кваліфікації.
- У нас було проведено не менше одного заходу на цю тему.
- Колеги пропонували керівництву обговорити цю тему.
- Тема ще не розглядалася.

ДОДАТОК В

Довідки про впровадження результатів дослідження

КОМУНАЛЬНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ
«ДНІПРОВСЬКА АКАДЕМІЯ НЕПЕРЕРВНОЇ ОСВІТИ»
ДНІПРОПЕТРОВСЬКОЇ ОБЛАСНОЇ РАДИ»
КОД ЄДРПОУ 41682253
вул. Володимира Антоновича, 70, м. Дніпро, 49006, тел/факс 056) 732-48-48
e-mail: kzvo@dano.dp.ua www.dano.dp.ua

«01» 12. 2025 № 674

Довідка
про впровадження результатів дисертаційного дослідження
аспіранта Чорноморського національного університету імені Петра Могили Атанасова Миколи Віталійовича
на тему «Управління персоналом на державній службі у вимірах взаємодії в кіберпросторі»,
на здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування» (галузь знань 28 «Публічне управління та адміністрування»).

Теоретичні положення, які обґрунтовано в дисертаційній роботі, впроваджені в навчальний процес у ході підготовки фахівців за освітньо-кваліфікаційним рівням «магістр» за напрямом «Публічне управління та адміністрування» денної та заочної форми навчання при викладанні навчальних дисциплін «Кадрова політика та публічна служба», «Право в публічному управлінні», у Комунальному закладі вищої освіти «Дніпровська академія неперервної освіти» Дніпропетровської обласної ради».

Ректор, д. держ. упр., проф.
Заслужений працівник освіти України Віктор СИЧЕНКО

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ
(ДУІТЗ)
вул. Кузнечна, 1, м. Одеса, 65023, тел. (048) 705-03-33, факс (048) 705-04-31
http://www.suitt.edu.ua, e-mail: suitt@suitt.edu.ua код ЄДРПОУ 43997335

23.01.2025 № 01-22/32 На №_____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження Атанасова Миколи Віталійовича з теми «Управління персоналом на державній службі у вимірах взаємодії в кіберпросторі» (за спеціальністю «Публічне управління та адміністрування»)

В основу дисертації Миколи Атанасова покладено результати досліджень і розробок, що отримані автором за безпосередньої участі в науково-дослідній роботі, яка проводились в Державному університеті інтелектуальних технологій і зв'язку з теми «Крос-функціональний підхід щодо імплементації інструментарію кіберпсихології в концепцію когнітивного маркетингу» (ДР № 0124U004705), де автором було науково обґрунтовано теоретичні підходи, методи та моделі взаємодії в кіберпросторі, а також акцентовано увагу на роль кіберхейту як складової частини кібербулінгу в системі розвитку персоналу на публічній службі.

Результати дисертаційного дослідження М. Атанасова були враховані при розробці навчальних курсів (обов'язкових компонент – далі ОК) освітньо-професійної програми «Публічне управління інформаційними та інноваційними екосистемами» для здобувачів першого (бакалаврський) рівня вищої освіти зі спеціальності 281 Публічне управління та адміністрування, а саме:

ОК-15 *Публічна служба*, де використані аналітичні матеріали щодо основних концепцій та шкіл управління персоналом; методології управління персоналом в органах публічної влади; принципів та методи управління персоналом у публічній службі, а також сучасних технологій вироблені HR-стратегії органів публічної влади;

ОК-18 *Управління персоналом у публічній службі* – враховано висновки автора про необхідність розгляду в даному курсі питання «Кіберпсихологічна компетентність у вимірах кар'єрного потенціалу публічних службовців», дана тема висвітлюється на лекційних (2 год.) та практичних (2 год) заняттях.

ОК-25 *Соціальна психологія* – в межах Теми 2 «Соціально-психологічні закономірності спілкування та взаємодії людей» використані результати проведеного у 2024 році емпіричного дослідження, зокрема застосовано

висновки щодо сучасного стану готовності державних службовців до професійної діяльності в кіберпросторі, а також визначено чинники, що впливають на професійну діяльність державних службовців у кіберпросторі.

На наш погляд, найбільш значущими результатами дослідження М. В. Атанасова є експериментально доведені факти про стан готовності сучасних державних службовців до професійної діяльності в кіберпросторі, а саме: лише у 14,7% державних службовців констатовано високий рівень готовності до професійної діяльності в кіберпросторі; у 53,9% – мінімально достатній для виконання професійних обов'язків; у 31,4% – незадовільний, що вказує на поширення діджитал-прокрастинації як деструктивного чинника, що знижує продуктивність та ускладнює самоменеджмент державного службовця. Автором дисертації також доведено, що професійна активність державних службовців у цифровому середовищі супроводжується як новими можливостями для ефективної професійної комунікації, так і зростанням соціальних ризиків, насамперед – кіберзалякуванням, кіберхейтом, прокрастинацією та цифровою втомою.

Отже, вважаємо доцільним використання результатів дисертаційного дослідження Атанасова Миколи Віталійовича з теми «Управління персоналом на державній службі у вимірах взаємодії в кіберпросторі» не лише в системі фахової підготовки публічних службовців але і в органів державної влади, зокрема при проведені щорічного оцінювання державних службовців.

Ректор Олександр Назаренко

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

DAAD
Deutscher Akademischer Austausch Dienst
German Academic Exchange Service

ДОВІДКА

про впровадження результатів дисертаційного дослідження Атанасова Миколи Віталійовича з теми «Управління персоналом на державній службі у вимірах взаємодії в кіберпросторі» (за спеціальністю «Публічне управління та адміністрування»)

Атанасова Микола Віталійович в якості експерта брав участь у проведенні досліджень та розробки практичних рекомендацій в міжнародних проєктах Німецької служби академічних обмінів, а саме:

1) «Навігація в цифровому просторі: стратегії підтримки молоді з урахуванням конфліктів» (DAAD-2024, ID-57709682), де автором обґрунтовано типові навігаційні маршрути в кіберпросторі, та чинники, що впливають на вибір молоддю цих маршрутів;

2) «Разом проти ненависті в Інтернеті: попередження та стратегії впливу на молодь в Німеччині, Киргизії, Молдові та Україні» (DAAD-2025, ID-57761453) – автором розроблено тренінгову програму для молодих публічних службовців, журналістів та інших фахівців соціономічної сфери «Пропедевтика кіберхейту та кібербулінгу у сфері публічного управління та адміністрування».

М. Атанасов є співавтором колективної монографії з теми «Кіберпсихологія у вимірах сучасного наукового дискурсу» (2024 р.) та двох наукових статей (Атанасов М. В. Роль кіберхейту як складової частини кібербулінгу у системі розвитку персоналу на публічній службі. *Публічне управління та регіональний розвиток*. 2025. № 28. С. 606–627; Атанасов М. В. Удосконалення компетентностей публічних службовців щодо управління місцевим розвитком на засадах процесного менеджменту. *Публічне управління та регіональний розвиток*. 2024. № 24. С. 937–963) виданих у фахових виданнях з публічного управління та адміністрування, де оприлюднені найбільш актуальні питання дисертаційної роботи.

Отже, вважаємо доцільним використання результатів дисертаційного дослідження Атанасова Миколи Віталійовича з теми «Управління персоналом на державній службі у вимірах взаємодії в кіберпросторі» та рекомендуємо їх поширення в практичну діяльність публічних службовців.

Керівник
української проєктної команди,
д. н. держ. упр., професор Світлана Хаджирадєва