

DOI 10.34132/pard2025.29.17

Отримано: 3 березня 2025
Змінено: 28 квітня 2025
Прийнято: 28 травня 2025
Опубліковано:
30 вересня 2025

Received: 3 March 2025
Revised: 28 April 2025
Accepted: 28 May 2025
Published:
30 September 2025

Mykola Atanasov

ANALYSIS OF WORLD EXPERIENCE IN THE FIELD OF IMPROVING THE PROCESS OF INTERACTION OF CIVIL EMPLOYEES IN CYBERSPACE

In this article, the author analyzes world experience in the field of improving the process of interaction of civil servants in cyberspace, which consists in analyzing social engineering, which is presented as an effective mechanism for influencing the formation, regulation and development of digital behavior of public servants. The essence of which is the conscious use of psychological, communicative and social tools aimed at adapting personnel to the digital environment, establishing the principles of digital ethics and reducing the level of cyber threats.

It is noted that social engineering can be considered, in particular, as a tool for transforming personnel policy, and involve the use of socio-psychological mechanisms for modeling the behavior of civil servants.

The author emphasizes that the digital behavior of civil servants is largely shaped by established or informal standards that operate within the professional community.

The experience of various countries (Singapore, Denmark, Canada, Estonia, Bulgaria, the Netherlands, the United Kingdom, etc.) on the issue of regulating the digital behavior of civil servants is analyzed, which showed that the comparative analysis of national approaches to regulating the digital behavior of civil servants made it possible to identify both common principles and specific features of different countries. Key among them are ethical governance, transparency, accountability,

respect for human rights and the development of digital competence in the public sector.

The conclusion is made that international practice demonstrates the multi-vector nature of approaches to the formation of ethical behavior of civil servants in the digital space.

Based on the analyzed international experience, it is advisable to introduce a phased model of digital ethics in the civil service in Ukraine, focusing on the successful practices of the above-mentioned countries.

Keywords: *social engineering, ethical behavior, civil servant, digital space, code of ethics, cyberspace, digital behavior.*

Постановка проблеми у загальному вигляді. У системі публічного управління соціальну інженерію доцільно розглядати як ефективний механізм впливу на формування, регулювання та розвиток цифрової поведінки публічних службовців. Її сутність полягає у свідомому застосуванні психологічних, комунікативних і соціальних інструментів, спрямованих на пристосування персоналу до цифрового середовища, утвердження принципів цифрової етики та зниження рівня кіберзагроз.

У традиційному трактуванні термін «соціальна інженерія» зазвичай асоціюється з кібератаками, що базуються на маніпуляції людською поведінкою з метою отримання доступу до конфіденційних даних. У цьому контексті соціальна інженерія розглядається як один із головних факторів ризику для кібербезпеки, оскільки зловмисники використовують психологічні прийоми, апелюючи до емоцій користувачів — страху, довіри чи поспіху — задля досягнення власних цілей [12; 20].

Водночас, як демонструє досвід Behavioural Insights Team (BIT) у Великій Британії, подібні механізми можуть бути переосмислені й використані у конструктивний спосіб, зокрема для підвищення ефективності управлінських процесів та удосконалення організаційної культури у державному секторі. Одним із ключових інструментів BIT є технологія «nudge» («м'яке підштовхування»),

що передбачає ненав'язливе спрямування поведінки працівників шляхом коригування архітектури вибору або зміни інформаційного контексту. Такі підходи довели свою дієвість у підвищенні виконавчої дисципліни, дотриманні етичних норм та запобіганні конфліктним ситуаціям у публічній службі [4].

Формулювання цілей статті (постановка завдання).

Метою статті є проаналізувати кращі зарубіжні практики у сфері моделювання цифрової поведінки, та практичні приклади ефективного застосування технологій поведінкового моделювання в середовищі державних службовців та обґрунтувати роль цих факторів у досліджуваній проблемі зокрема в розрізні застосування зазначених інструментів у вітчизняній практиці розбудови державної служби.

Виклад основного матеріалу дослідження. На думку Світового банку, соціальна інженерія може бути ефективним інструментом протидії корупції та недоброчесним практикам у системі державного управління. Це досягається завдяки цілеспрямованому формуванню соціальних установок і поведінкових моделей, розвитку організаційної культури доброчесності, запровадженню прозорих процедур ухвалення рішень та інтеграції поведінкових інтервенцій у систему 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. Айзенем [3]. Згідно з цією теорією, реальна поведінка індивіда визначається його намірами, які, у свою чергу, формуються під впливом трьох основних чинників які представлені на рис .1.

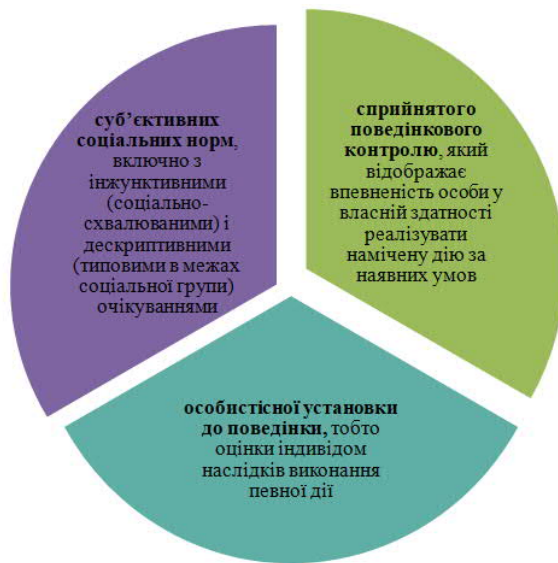


Рис. 1. Основні чинники Теорії запланованої поведінки за І. Айзенем.
Джерело: сформовано автором на основі: [3].

У сфері публічного управління особливого значення набуває компонент соціальних норм, оскільки цифрова поведінка державних службовців значною мірою формується під впливом усталених або неформальних стандартів, що функціонують у межах професійної спільноти. Як підкреслюють фахівці у галузі поведінкових наук, групові норми та колективні установки виступають важливим чинником регулювання індивідуальної поведінки, сприяючи її спрямуванню у бік більш відповідального, етичного та безпечного цифрового самовираження [5].

Отже, застосування теорії запланованої поведінки (Theory of Planned Behavior, TPB) у контексті державної служби відкриває можливості не лише для діагностики існуючих моделей поведінки, але й для розроблення цілеспрямованих поведінкових інтервенцій, орієнтованих на трансформацію установок і соціальних норм. Такий підхід сприяє формуванню стійких практик етичної, безпечної та добросовісної 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 наступних компонентів які представлені на рис. 2.



Рис. 2. Компоненти механізму моделювання етичної поведінки.
Джерело: сформовано автором

Згідно з результатами сучасних досліджень, соціальні норми демонструють найвищу ефективність тоді, коли вони комунікуються через інформування про поведінку більшості або референтної групи – «типових колег» чи «переважної частини спільноти» [4]. Подібний підхід було апробовано в низці емпіричних досліджень.

Так, у Німеччині надання домогосподарствам порівняльної інформації про рівень споживання електроенергії у співвідношенні з середніми показниками по сусідству спричинило суттєві зміни поведінки у напрямі більш ощадного використання ресурсів [5].

У сфері цифрової поведінки державних службовців механізм «підштовхування соціальних норм» (social norms nudging) може бути реалізований через впровадження візуалізованих етичних орієнтирів, демонстрацію позитивних кейсів або соціальні комунікаційні кампанії, спрямовані на популяризацію доброчесної цифрової взаємодії в межах державних органів. Такий підхід сприяє формуванню ефекту соціального тиску та конформності, який стимулює добровільне дотримання етичних стандартів без застосування жорстких адміністративних заходів впливу.

Застосування технології «підштовхування соціальних норм» у системі державної служби України може стати ефективним інструментом формування нової організаційної культури цифрової доброчесності. Такий підхід забезпечує поступову трансформацію поведінкових моделей державних службовців, підвищує відповідальність та усвідомлення етичних аспектів цифрової взаємодії, а також зменшує потребу у примусових регулятивних механізмах. У довгостроковій перспективі це сприятиме становленню етичного цифрового середовища в державному секторі та зміцненню довіри громадян до публічних інституцій.

3. Також у сучасних підходах до управління поведінкою персоналу дедалі більшого значення набуває концепція «advisory nudging» («консультативне або порадицьке 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 [22].

У сфері державного управління, зокрема в HR-контексті, такий підхід має потенціал для формування етичної цифрової поведінки, оскільки реалізується шляхами які представлені на рис. 3.



Рис. 3. Шляхи формування етичної цифрової поведінки.
Джерело: сформовано автором

Практичні приклади ефективного застосування технологій поведінкового моделювання спостерігаються, зокрема, у Сінгапурі та Данії, де концепція «консультативного підштовхування» активно використовується у рамках державних програм із розвитку цифрової етики та професійного удосконалення державних службовців [5; 6].

Так, у Сінгапурі в межах урядової кампанії «Sustainability Starts with Me» працівники Міністерства навколишнього середовища впроваджували індивідуальні «зони сортування відходів» та створювали нагадування наприкінці робочого дня, які виконували функцію «самопідказок» (self-nudge), стимулюючи сталі екологічні звички — зокрема, сортування сміття та очищення упаковок перед утилізацією. Подібні інтервенції демонструють, що поведінкові зміни можуть досягатися без примусу, виключно за рахунок формування внутрішньої відповідальності та усвідомлення соціальної значущості дій [19].

Крім того, Міністерство праці Сінгапуру (MOM) запровадило оновлений формат комунікацій із роботодавцями, спрямований на

підвищення рівня дисципліни щодо сплати обов'язкових внесків. Зокрема, було спрощено текст повідомлень, додано соціальне порівняння («96% роботодавців сплачують внески вчасно»), а також змінено колір листів на рожевий, що створювало ефект візуального виділення та емоційного залучення. Унаслідок цього було зафіксовано зростання рівня своєчасної сплати внесків на 3–5 % порівняно з попередньою кампанією [21].

У 2002 році в Данії було засновано MindLab — інноваційну урядову лабораторію, створену при кількох міністерствах, яка стала однією з перших платформ, орієнтованих на застосування дизайн-мислення, поведінкового моделювання та прототипування у сфері публічного управління. Хоча діяльність MindLab не повністю відповідає класичній моделі «nudge», її методологічна база, що передбачає тестування поведінкових сценаріїв, аналіз соціальних впливів та моделювання реакцій користувачів, корелює з концепцією «консультативного підштовхування» [21].

Одним із прикладів практичного застосування цього підходу є створення комунікаційного простору для обговорення принципів цифрової етики серед державних службовців, що сприяє закріпленню етичних норм у їхній повсякденній професійній діяльності. Подібна практика була реалізована податковим агентством SKAT, яке замість традиційних бюрократичних інструктажів започаткувало формат зустрічей стартапів із досвідченими підприємцями, використовуючи соціальний приклад як чинник підвищення довіри та мотивації [7].

Офіційне кейс-дослідження компанії Pensaki також демонструє ефективність цієї методології: під час кампанії іпотечного кредитування BRF-Kredit було зафіксовано понад 90% позитивних відгуків завдяки використанню персоналізованих листів у ручних конвертах без логотипів, що знижувало психологічний бар'єр у клієнтів із фінансовими труднощами [20]. Такий підхід можна розглядати як етично орієнтований механізм комунікації, який принципово відрізняється від формалізованого адміністративного листування та сприяє підвищенню довіри до державних інституцій.

Отже, аналіз зарубіжного досвіду засвідчує, що використання технологій поведінкового моделювання, зокрема інструментів «м'якого підштовхування» (nudge), є результативним механізмом трансформації професійної поведінки державних службовців. На відміну від директивних або репресивних управлінських практик, даний підхід ґрунтується на принципах поваги до автономії особистості та передбачає етичну орієнтацію на добровільний вибір у межах раціонально структурованого інформаційного середовища. Така модель сприяє внутрішній мотивації до зміни поведінки й підвищує рівень відповідальності державних службовців за власні дії у цифровому просторі.

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 реалізувати етапи які зображені на рис. 4.



Рис. 4. Етапи реалізації технологій поведінкового моделювання.
Джерело: сформовано автором

Можемо констатувати що, впровадження концепції «м'якого підштовхування» у систему державного управління створює передумови для підвищення ефективності формування цифрової культури поведінки державних службовців. Реалізація цього підходу в українській публічній службі є перспективним напрямом модернізації управлінських практик, який дозволяє без застосування надмірного адміністративного контролю забезпечити становлення етично виваженого, соціально відповідального та проактивного цифрового середовища.

Водночас, із посиленням ролі цифрових платформ у функціонуванні державного сектору та зростанням кіберзагроз, питання цифрової етики набуває ключового значення для ефективності та безпеки публічного управління. У цьому контексті Цифровий етичний кодекс розглядається як нормативно-правовий інструмент регулювання поведінки державних службовців у кіберпросторі, що охоплює професійну взаємодію через соціальні мережі, електронну пошту, месенджери та інші комунікаційні засоби. Запровадження такого кодексу сприяє підтриманню балансу між професійною відповідальністю, інформаційною безпекою та дотриманням прав громадян, забезпечуючи етичну стабільність цифрового публічного простору.

У світовій практиці цифрові етичні кодекси (Digital Ethics Codes) розглядаються як невід'ємний елемент політики належного врядування (good governance), що ґрунтується на принципах прозорості, підзвітності та поваги до приватності в цифровому середовищі.

Згідно з документом Організації економічного співробітництва та розвитку (OECD) «Рамки політики цифрового урядування» (Digital Government Policy Framework, 2020), етичність, прозорість і доброчесність визначаються як базові засади формування довіри між державними службовцями та громадянами [17]. У межах цих підходів OECD рекомендує державам інтегрувати етичні стандарти у процес цифрової трансформації, що охоплює, зокрема, боротьбу з дезінформацією, забезпечення відкритості управлінських процесів та захист персональних даних [17; 16].

Водночас, Європейська Комісія у стратегічному документі «Цифровий компас 2030» (Digital Compass 2030, 2021) наголошує на необхідності дотримання фундаментальних цифрових прав і принципів, серед яких — прозорість, участь громадян у прийнятті рішень, інклюзивність та захист від цифрової агресії. У документі окреслено напрям державної політики, спрямований на підвищення рівня довіри до процесів цифрової трансформації та етичного врядування у цифровому середовищі [9].

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) [15]. Цей документ є частиною ширшої етики публічної служби та має нормативно-роз'яснювальний характер, та вирізняється широкою сферою впливу (завданнями) які представлено на рис. 5.

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.



Рис. 5. Головні завдання Кодексу поведінки щодо використання соціальних мереж Нідерландів.

Джерело: сформовано автором на основі: [15].

«Рекомендації щодо соціальних мереж для державних службовців» є офіційною позицією уряду щодо того, як державні службовці повинні поводитися в соціальних мережах, включаючи особисті акаунти [11]. Ключові принципи згадуваних рекомендацій представлено нами на рис. 6.

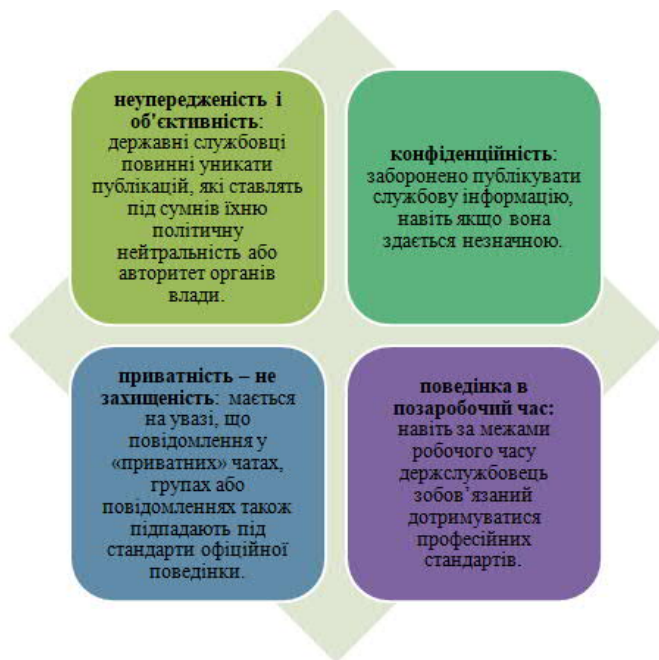


Рис. 6. Ключові принципи «Рекомендації щодо соціальних мереж для державних службовців».

Джерело: сформовано автором на основі: [11].

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, що включає наступні складові які презентовано на рис. 7.



Рис. 7. Концепція SAFE: базові складові
Джерело: сформовано автором на основі [11].

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 реалізації наступних завдань що репрезентовано нами на рис.8.

Документ підкреслює, що навіть у публічних суперечках державний службовець має діяти стримано, доброзичливо і професійно [11].



Рис. 8. Перелік завдань для реалізації Digital communication
Джерело: сформовано автором

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 [11]. 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 [14].

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 [13]. 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 [14].

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 [9].

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 [13].

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) [8], 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 [8].

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. [10].

Кодекс визначає ключові етичні принципи, обов'язкові для службовців що агреговано на рис. 9.

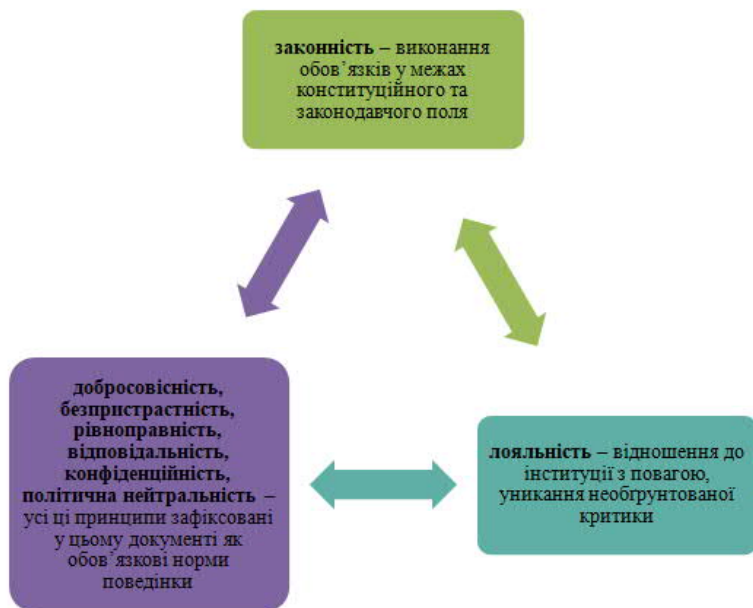


Рис. 9. Ключові (обов'язкові) етичні принципи кодексу.
Джерело: сформовано автором

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

Чл.17(1-2) – державні службовці 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 [1; 2].

У лютому 2021 року уряд Індії впровадив комплекс нових правил, покликаних забезпечити етичну поведінку онлайн-платформ та цифрових медіа [21]. Журнали та інтернет-посередники (соціальні мережі, новинні ресурси, OTT сервіси) отримали чіткі обов’язки щодо контролю контенту, відповідальності за нього та підтримки користувачьких 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 [21].

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 саморегулювального органу (Self-Regulating Body). Якщо скаржник не задоволений відповіддю або її відсутністю, він може звернутися до зареєстрованого саморегулювального 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 [21].

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 [18].

Таким чином, автоматизовані системи розглядаються не як замітники, 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.

Отже модель Індії у сфері цифрового врядування демонструє поєднання горизонтальної та вертикальної інтеграції механізмів контролю за онлайн-контентом, забезпечуючи баланс між саморегуляцією, галузевим наглядом та державним регулюванням. Такий підхід відображає комплексну модель управління цифровою екосистемою, що включає міжвідомчу координацію, прозорі стандарти публікацій та систему обов'язкової етики для великих цифрових платформ. Важливим елементом цієї моделі є механізм розгляду скарг та інститут офіцерів відповідальності, який дозволяє забезпечувати рівновагу між свободою висловлювань і захистом прав користувачів.

Узагальнення порівняльного аналізу національних підходів до регулювання цифрової поведінки державних службовців дає змогу виокремити як спільні принципи, так і специфічні особливості різних країн. Серед них ключовими є етичне врядування, прозорість, підзвітність, дотримання прав людини та розвиток цифрової компетентності в публічному секторі.

В українському контексті формування цифрових етичних стандартів державної служби поки що не набуло завершеного інституційного оформлення. Водночас результати емпіричного дослідження, наведені у попередньому розділі, засвідчують наявність проблемних аспектів у цифровій поведінці державних службовців — від розмиття меж між професійною та особистою комунікацією в онлайн-просторі до високого рівня толерантності до агресії,

прокрастинації та неетичних проявів у цифровому середовищі. Це підкреслює необхідність розроблення цілісної політики цифрової етики в державному управлінні України.

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 [17].

Варто зазначити, що міжнародна практика демонструє багатовекторність підходів до формування етичної поведінки державних службовців у цифровому просторі.

Виходячи з проаналізованого міжнародного досвіду в Україні доцільно запровадити поетапну модель цифрової етики на державній службі, орієнтуючись на успішні практики вище зазначених країн.

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 проведеного безпосередньо автором цієї статті: 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.

Висновки. 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.

Таким чином, впровадження корпоративного цифрового етичного кодексу в Україні, із урахуванням провідних міжнародних практик, може стати ключовим чинником формування безпечної, доброчесної та відповідальної поведінки державних службовців у цифровому середовищі. Такий документ виступатиме не лише регулятивним інструментом, але й механізмом інституціоналізації нової цифрової культури державної служби в умовах становлення кіберсоціального суспільства.

Водночас цифрові етичні кодекси мають виконувати функцію не лише формального нормативного регламенту, а й інструменту розвитку професійної культури цифрової комунікації у публічному секторі. Їх імплементація сприятиме зміцненню суспільної довіри до державної служби, підвищенню ефективності реалізації політики кібербезпеки, а також гармонізації міжособистісної взаємодії у цифровому просторі. У довгостроковій перспективі це створить передумови для формування етичного, стійкого та безпечного цифрового урядування в Україні.

АНАЛІЗ СВІТОВОГО ДОСВІДУ У СФЕРІ УДОСКОНАЛЕННЯ ПРОЦЕСУ ВЗАЄМОДІЇ ДЕРЖАВНИХ СЛУЖБОВЦІВ У КІБЕРПРОСТОРІ

У данні статті автором зроблено аналіз світового досвіду у сфері удосконалення процесу взаємодії державних службовців у кіберпросторі якій полягає у аналізі соціальної інженерії яка презентована як ефективний механізм впливу на формування, регулювання та розвиток цифрової поведінки публічних службовців. Сутність якої полягає у свідомому застосуванні психологічних, комунікативних і соціальних інструментів, спрямованих на пристосування персоналу до цифрового середовища, утвердження принципів цифрової етики та зниження рівня кіберзагроз.

Зазначено що соціальна інженерія може розглядатися зокрема і як інструмент трансформації кадрової політики, і передбачати застосування соціально-психологічних механізмів для моделювання поведінки державних службовців.

Автором наголошено що цифрова поведінка державних службовців значною мірою формується під впливом усталених або неформальних стандартів, що функціонують у межах професійної спільноти.

Проаналізовано досвід різних країн (Сінгапуру, Данії, Канади, Естонії, Болгарії, Нідерландів, Великобританії та ін.) щодо питання врегулювання цифрової поведінки державних службовців які засвідчили що здійснений порівняльний аналіз національних підходів до регулювання цифрової поведінки державних службовців дав змогу виокремити як спільні принципи, так і специфічні особливості різних країн. Серед них ключовими є етичне врядування, прозорість, підзвітність, дотримання прав людини та розвиток цифрової компетентності в публічному секторі.

Зроблено висновок що міжнародна практика демонструє багатовекторність підходів до формування етичної поведінки державних службовців у цифровому просторі.

Виходячи з проаналізованого міжнародного досвіду в Україні доцільно запровадити поетапну модель цифрової етики на

державній службі, орієнтуючись на успішні практики вище зазначених країн.

Ключові слова: соціальна інженерія, етична поведінка, державний службовець, цифровий простір, етичний кодекс, кіберпростір, цифрова поведінка.

Author Contributions: Conceptualization, M.A; Writing – original draft, M. A; Writing – review & editing, M. A. Author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable as study did not include human subjects.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Министерството на вътрешните работи. Етичен кодекс за поведение на държавните служители в Министерството на вътрешните работи. (n.d.). (2020). www.legal-tech.bg Retrieved from: https://legal-tech.bg/featured_item/kodeks-za-povedenie-na-sluzhitelite-v-drzhavnata-administratsiya/ [in Bulgarian].
2. Министерството на вътрешните работи. Заповед № 81213-1169 от 23 август 2024 г. Относно изменение и допълнение на етичния кодекс за поведение на държавните служители в Министерството на вътрешните работи. (n.d.). (2024). www.lex.bg/ Retrieved from: https://lex.bg/bg/laws_stoyan/ldoc/2137245285 [in Bulgarian].
3. Ajzen, I., (1991). The Theory of Planned Behavior // *Organizational Behavior and Human Decision Processes*.. 50(2), (pp.179–211). Retrieved from: [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T) [in English].
4. Behavioural Insights Team. (n.d.). (2019). www.bi.team Retrieved from: <https://www.bi.team/> [in English].

5. Burger, A., Schubert, C., & Bizer, K. (2015). Nudging for Sustainability: The Use of Behavioural Economics in Environmental Policy. *Oxford Journal of Economic Policy*. 31(2), (pp. 231–252). [in English].
6. Indian School of Business Executive Education (ISB ExecEd). (n.d.). (2023). Behavioural Insights for Public Sector Leaders. www.execed.isb.edu. Retrieved from: <https://execed.isb.edu>. [in English].
7. Danish business tax affairs. (n.d.). (2025). www.skat.dk Retrieved from: <https://skat.dk/en-us/individuals> [in English].
8. Department of Finance (Ireland). (n.d.). (2004). www.circulars.gov. Civil Service Code of Standards and Behaviour: Circular 26/2004. Retrieved from: <https://circulars.gov.ie/pdf/circular/finance/2004/26.pdf> [in English].
9. Estonian Government Office. E-Governance and Digital Communication Policy Guidelines. (n.d.). (2022). www.scribd.com Retrieved from: <https://www.scribd.com/document/671607084/Estonia-E-Gov-Survey-MSQ-2022>. [in English].
10. 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*. 33(7), (2020). www.ipa.government. Retrieved from: <https://www.ipa.government>. bg/bg/novini/priet-e-nov-kodeks-za-povedenie-na-sluzhitelite [in English].
11. Government Communication Service. Digital communication. (n.d.). (2020). www.gcs.civilservice.gov. Retrieved from: <https://gcs.civilservice.gov.uk/guidance/digital-communication/> [in English].
12. Hatfield, J. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, (pp.102–113). [in English].
13. Kalvet, T. (2012). Innovation: A factor explaining e-government success in Estonia // *Electronic Government, an International Journal*, 9(2), (pp.142–157). [in English].
14. Ministry of Finance of Estonia. Code of ethics for officials. Ethics Council of Public Service, (n.d.). www.fin.ee (2017). Retrieved from: <https://www.fin.ee/en/media/2195/download> [in English].
15. 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, (n.d.). www.government.nl (2011). Retrieved from: <https://www.government.nl/documents/publications/2011/12/01/code-of-conduct-for-the-use-of-social-media-by-civil-servants> [in English].
16. OECD. Good Practice Principles for Data Ethics in the Public Sector. Paris : OECD Publishing, (n.d.). www.oecd.org (2021). Retrieved from: <https://www.oecd.org>

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 [in English].

17. OECD. OECD Public Integrity Handbook. Paris : OECD Publishing, (n.d.). [www.oecd.org](https://www.oecd.org/en/publications/oecd-public-integrity-handbook_ac8ed8e8-en.html) (2020). Retrieved from: https://www.oecd.org/en/publications/oecd-public-integrity-handbook_ac8ed8e8-en.html [in English].

18. Mendiratta, R. (2021). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, Retrieved from: <https://wilmap.stanford.edu/entries/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021> [in English].

19. Lim, C. (2022). Sustainability as Behavioural Change: Nudging the Good, Discouraging the Bad // *ETHOS*, 24. Institute of Governance and Policy, Civil Service College. Retrieved from: <https://knowledge.csc.gov.sg/ethos-issue-24/sustainability-as-behavioural-change-nudging-the-good-discouraging-the-bad>. [in English].

20. Mouton, F., Nottingham, A., Leenen, L., & Venter H. (2018). Finite state machine for the social engineering attack detection model: SEADM. *SAIEE Africa Research Journal*, 109(2), Retrieved from: https://scielo.org.za/scielo.php?pid=S1991-16962018000200004&script=sci_arttext. [in English].

21. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. (n.d.). (2021). www.meity.gov.in. Retrieved from: <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>. [in English].

22. Ethical Persuasion and Behavioural Public Policy *SAGE Journals* (2021). (n.d.). www.journals.sagepub.com Retrieved from: <https://journals.sagepub.com/> [in English].

Відомості про автора / Information about the Author

Микола Атанасов, завідувач навчально-наукової лабораторії дистанційної та он-лайн освіти, Державного університету інтелектуальних технологій і зв'язку, м. Одеса, Україна. E-mail: nkl.atnsv@gmail.com, orcid: <https://orcid.org/0000-0002-9061-6858>.

Mykola Atanasov, Head of the Educational and Scientific Laboratory of Distance and Online Education, State University of Intellectual

al Technologies and Communications, Odessa, Ukraine. E-mail: nkl.atnsv@gmail.com, orcid: <https://orcid.org/0000-0002-9061-6858>.

Atanasov, M. (2025). Analysis of world experience in the field of improving the process of interaction of civil employees in cyberspace. *Public Administration and Regional Development*, 29, 1073-1101, <https://doi.org/10.34132/pard2025.29.17>