

5. Непомнящий О. М. Стан та перспективи організаційно-правового забезпечення діяльності інженера-консультанта в Україні / О. М. Непомнящий, І. В. Хараїм [Електронний ресурс]. *Державне управління, удосконалення та розвиток*. № 2. 2018 р. URL: http://www.dy.nayka.com.ua/pdf/2_2018/5.pdf

6. Непомнящий О. М. Інженер-консультант у системі господарської і професійної діяльності в Україні. *Інвестиції: практика та досвід*. 2018. № 9. URL: http://www.investplan.com.ua/pdf/9_2018/20.pdf

DOI <https://doi.org/10.36059/978-966-397-466-8-14>

РИЗИКИ НЕТОКРАТИЗАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ

Стороженко Л. Г.

*кандидат філологічних наук, доцент,
докторант кафедри публічного управління та адміністрування
Навчально-наукового інституту менеджменту та підприємництва
Державного університету інформаційно-комунікаційних технологій
м. Київ, Україна*

У контексті впливу глобалізації на формування сучасного державного управління, нетократизація постає закономірним явищем, що відображає прагнення до використання сучасних інформаційно-комунікаційних технологій для розширення участі громадян у процесах прийняття рішень на державному рівні, що, у свою чергу, сприяє підвищенню легітимності та ефективності демократичних інститутів [1].

Однак поряд з прогресивною інтеграцією органами управління сучасних цифрових технологій з метою підвищення якості та ефективності державного управління, можна виокремити низку ризиків, зумовлених нетократичними процесами, серед яких:

– кібербезпека (збільшення можливостей кібератак та порушення конфіденційності даних може призвести до витоку важливої інформації, впливу на результати прийняття рішень тощо);

– нерівність доступу (використання сучасних цифрових технологій може підсилити нерівність у доступі до інформації та участі громадськості в управлінських процесах (громадяни, які мають доступ до новітніх технологій та знань, можуть мати перевагу перед представниками суспільства, які не мають такого доступу));

– цифрова дискримінація (розвиток нетократичних методів управління може призвести до виникнення цифрової дискримінації (грома-

дяни, які не мають навичок у використанні інформаційно-комунікаційних технологій або вільного доступу до них, відчують себе «виключеними» з управлінських процесів));

- цифрова неграмотність (відставання окремих груп населення у цифровій грамотності може призвести до ще більшого «виключення» їх з процесів управління);

- втрата особистості (збільшення автоматизації та використання нетократичних управлінських алгоритмів може призвести до втрати індивідуалізації в управлінні, що суттєво знижує рівень довіри громадян до управлінських структур);

- втрата приватності (збір і обробка великих обсягів даних для прийняття управлінських рішень може порушувати приватність громадян);

- маніпуляція інформацією (використання нетократичних алгоритмів управління та штучного інтелекту для аналізу даних може призвести до маніпулювання даними та їх спотворення з політичною або особистою метою);

- втрата контролю (занадто велика автоматизація процесів управління може призвести до втрати контролю над цими процесами та зниження прозорості управління);

- збільшення нерівності: у разі неадекватної імплементації цифрових технологій може збільшитися рівень нерівності між країнами та в межах однієї країни;

- залежність від технологій (залежність від цифрових технологій може зробити управлінські структури більш вразливими у разі технічних неполадок або атак).

Зазначені ризики, звичайно, вимагають впровадження ефективних безпекових заходів і захисту прав громадян.

Крім окреслених викликів, можна визначити низку глобалізованих проблеми, зумовлених нетократизацією державного управління:

- недостатня демократична легітимність (збільшення впливу цифрових технологій може призвести до зростання влади технократів, що може підірвати демократичну легітимність уряду та управлінських органів);

- зменшення прозорості та відповідальності (автоматизація управлінських процесів може призвести до труднощів у визначенні, хто несе відповідальність за прийняття рішень та за їхні наслідки, що може призводити до корупції та зловживання владою);

- загроза державному суверенітету (використання зовнішніх цифрових платформ та послуг може призвести до порушення національного суверенітету та контролю над власними даними та інформацією);

– недостатність управління змінами (впровадження нетократичних методів управління може призвести до нестабільності та опору з боку традиційних урядових структур, які не готові або не можуть адаптуватися до роботи з новітніми інформаційно-комунікаційними технологіями);

– нерівновага у розподілі ресурсів (неоднаковий доступ до цифрових технологій та послуг зумовлює зростання нерівності у суспільстві та призводить до виникнення соціальних та економічних проблем тощо).

Зазначені ризики підкреслюють необхідність уважного та комплексного підходу до впровадження нетократичних методів управління та постійного моніторингу їхніх наслідків.

Для зменшення цих ризиків важливо впроваджувати ефективні заходи кібербезпеки, забезпечувати доступ до технологій для всіх верств суспільства, проводити освітні кампанії щодо цифрової грамотності та забезпечувати прозорість і відкритість у процесах управління тощо.

Література:

1. Storozhenko L. H. Netocratic vector of formation of public administration in the information society. Modernization of the system of public management and administration in Ukraine: the experience of the Republic of Latvia. Riga, Latvia : Baltija Publishing, 2023. P. 99–114.

DOI <https://doi.org/10.36059/978-966-397-466-8-15>

БАЗОВІ ЧИННИКИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКОВОГО СЕРЕДОВИЩА В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Сухачов М. Р.

*аспірант науково-дослідного центру
Національного університету цивільного захисту України
м. Черкаси, Україна*

Воєнний стан в Україні, введений у відповідь на військову агресію з боку російської федерації, висвітлив критичну необхідність створення ефективного безпекового середовища. Безпека охоплює не лише оборону держави, але й стабільність внутрішньої системи публічного управління, громадське єднання та інноваційний розвиток. Важливо